53-1001160-02
March 9, 2009

Brocade M-EOS Command Line Interface

User Manual 9.9.2

BROCADE

Copyright © 2006-2009 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Fabric OS, File Lifecycle Manager, MyView, and StorageX are registered trademarks and the Brocade B-wing symbol, DCX, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication Number	Summary of Changes	Date
E/OS Command Line Interface User Manual	620-000134-000	Initial release of Manual	November 2001
E/OS Command Line Interface User Manual	620-000134-100	Updates for E/OS 2.0	May 2002
E/OS Command Line Interface User Manual	620-000134-200	Updates for E/OS 3.0	August 2002
E/OS Command Line Interface User Manual	620-000134-300	Updates for E/OS 4.0	September 2002
E/OS Command Line Interface User Manual	620-000134-400	Updates for E/OS 4.1	October 2002
E/OS Command Line Interface User Manual	620-000134-500	Updates for E/OS 4.1 CD-ROM final	October 2002
E/OS Command Line Interface User Manual	620-000134-600	Updates for E/OS 5.1 and EFCM 7.1	February 2003

Title	Publication Number	Summary of Changes	Date
E/OS Command Line Interface User Manual	620-000134-601	Updates for E/OS 5.5	July 2003
E/OS Command Line Interface User Manual	620-000134-700	Updates for E/OS 6.0	October 2003
E/OS Command Line Interface User Manual	620-000134-710	Updates for E/OS 6.1	December 2003
E/OS Command Line Interface User Manual	620-000134-720	Updates for E/OS 6.2	June 2004
E/OS Command Line Interface User Manual	620-000134-730	Updates for E/OS 7.0	December 2004
E/OS Command Line Interface User Manual	620-000134-740	Updates for E/OS 8.0	June 2005
E/OS Command Line Interface User Manual	620-000134-750	Corrections to manual	September 2005
E/OS Command Line Interface User Manual	620-000134-760	Updates for E/OS 8.2	April 2006
E/OS Command Line Interface User Manual	620-000134-770	Updates for E/OS 9.0	May 2006
E/OS Command Line Interface User Manual	620-000134-780	Updates for E/OS 9.1	September 2006
Brocade M-EOS Command Line Interface User Manual	53-1000642-01	Updates for M-EOS 9.6	June 2007
Brocade M-EOS Command Line Interface User Manual	53-1000642-02	Updates for M-EOS 9.7	March 2008
Brocade M-EOS Command Line Interface User Manual	53-1000642-03	Updates for M-EOS 9.8	July 2008
Brocade M-EOS Command Line Interface User Manual	53-1001160-01	Updates for M-EOS 9.9	November 2008
Brocade M-EOS Command Line Interface User Manual	53-1001160-02	Updates for M-EOS 9.9.2	March 2009

Contents

About This Document

In this chapter xv
How this document is organized xv
Supported hardware and software xvi
What's new in this document xvi
Document conventions xvii
Text formatting xvii
Command syntax conventions xvii
Notes, cautions, and warnings xviii
Key terms xviii
Additional information xviii
Brocade resources xviii
Other industry resources xix
Getting technical help xix
Document feedback xx

Chapter 1 Introduction

In this chapter 1
Command Line Interface overview 1
Entering Command Line Interface commands 1
Documentation conventions 2
Navigation conventions 2
Command tree 3
Navigation of the CLI command tree 10
Parameters 12
Output 12
Logging in and logging out 12
Types of users 12
Passwords and secrets 13
Globally available commands 13
login 13
logout 14
Using the commaDelim command 15
commaDelim 15
Handling CLI errors 16
Using CLI help 16
Commenting scripts 16
ED-5000 Director 17

Telnet session 18
Ethernet connection loss. 18

Chapter 2 CLI Commands

In this chapter 19

Command overview. 19

New and changed commands 19
Changed commands 19

config 19
config.alias 20
config.alias.activatePending 21
config.alias.add 21
config.alias.clearPending 22
config.alias.delete 22
config.alias.replacePending 23
config.alias.setCLIState 23
config.alias.setWebState 23
config.alias.showActive 24
config.alias.showPending 25
config.enterpriseFabMode.setState 25
config.features.enterpriseFabMode 26
config.features.ficonMS 27
config.features.installKey 27
config.features.NPIV 28
config.features.openSysMS 28
config.features.openTrunking 29
config.features.show 30
config.fencing 31
config.fencing.addPolicy 31
config.fencing.addPort. 31
config.fencing.deletePolicy 32
config.fencing.removePort. 33
config.fencing.setParams 34
config.fencing.setState 35
config.fencing.show 35
config.fencing.showTypeTable. 37
config.ficonCUPZoning. 37
config.ficonCUPZoning.addControlHost 37
config.ficonCUPZoning.deleteControlHost 38
config.ficonCUPZoning.setState 38
config.ficonCUPZoning.show. 39
config.ficonMS.setMIHPTO 40
config.ficonMS.setState 40
config.ficonMS.show 41
config.ip.ethernet. 42
config.ip.lineSpeed 42
config.ip.show 43
config.ip.v6. 44
config.NPIV 44
config.NPIV.maxPortIDs 45

config NPIV setALPAREstate 45
config.NPIV.setState 46
config.NPIV.show 46
config.NSTools 47
config.NSTools.clearSnapshot 47
config.NSTools.saveSnapshot 48
config.NSTools.showSnapDiff 48
config.NSTools.showSnapshot 49
config.openSysMS.setHostCtrlState 50
config.openSysMS.setState 50
config.port.blocked 51
config.port.fan 52
config.port.name 52
config.port.rxCredits 53
config.port.show 54
config.port.showPortAddr 56
config.port.showCredits 57
config.port.speed 58
config.port.swapPortByAddr 59
config.port.swapPortByNum 59
config.port.type 60
config.security 61
config.security.authentication.interface 61
config.security.authentication.interface.api.outgoing 61
config.security.authentication.interface.api.sequence 62
config.security.authentication.interface.cli.sequence 62
config.security.authentication.interface.eport.outgoing 63
config.security.authentication.interface.eport.sequence 64
config.security.authentication.interface.nport.outgoing 64
config.security.authentication.interface.nport.sequence 65
config.security.authentication.interface.osms.outgoing 66
config.security.authentication.interface.osms.setKey 66
config.security.authentication.interface.serial.enhancedAuth . 67
config.security.authentication.interface.show 67
config.security.authentication.interface.web.sequence 68
config.security.authentication.port.override 69
config.security.authentication.port.show 70
config.security.authentication.RADIUS 70
config.security.authentication.RADIUS.attempts 70
config.security.authentication.RADIUS.deadtime 71
config.security.authentication.RADIUS.deleteServer 72
config.security.authentication.RADIUS.server 72
config.security.authentication.RADIUS.show 73
config.security.authentication.RADIUS.timeout 74
config.security.authentication.switch.setSecret 75
config.security.authentication.user 75
config.security.authentication.user.add 75
config.security.authentication.user.delete 77
config.security.authentication.user.modify 77
config.security.authentication.user.passExpTime 78
config.security.authentication.user.role 79
config.security.authentication.user.show 79

config.security.fabricBinding 80
config.security.fabricBinding.activatePending 82
config.security.fabricbinding.addAttachedMembers 82
config.security.fabricBinding.addMember 83
config.security.fabricBinding.clearMemList 83
config.security.fabricbinding.deactivateFabBind 84
config.security.fabricBinding.deleteMember 84
config.security.fabricBinding.replacePending 85
config.security.fabricBinding.showActive 85
config.security.fabricBinding.showPending 86
config.security.portBinding 87
config.security.portBinding.bound 87
config.security.portBinding.show 88
config.security.portBinding.wwn 89
config.security.ssh 90
config.security.ssh.resetKeys 91
config.security.ssh.setRenegotiationMB 91
config.security.ssh.setState 92
config.security.ssh.show 92
config.security.switchAcl 93
config.security.switchAcl.addRange 93
config.security.switchAcl.deleteRange 94
config.security.switchAcl.setState 95
config.security.switchAcl.show 95
config.security.switchBinding 96
config.security.switchBinding.addMember 97
config.security.switchBinding.deleteMember 97
config.security.switchBinding.setState 98
config.security.switchBinding.show 98
config.security.ssl 99
config.security.ssl.generateKeys 99
config.security.ssl.resetKeys 100
config.security.ssl.setRenegotiationMB 101
config.security.ssl.setWebState 101
config.security.ssl.setAPIState 102
config.security.ssl.show 102
config.snmp 104
config.snmp.addAccessEntry 105
config.snmp.addAccessViews 105
config.snmp.addCommunity 106
config.snmp.addTargetParams 107
config.snmp.addUserEntry 108
config.snmp.addV3Group 109
config.snmp.addV1Target 110
config.snmp.addV2Target 111
config.snmp.addV3Target 112
config.snmp.authTraps 113
config.snmp.deleteAccessEntry 114
config.snmp.deleteCommunity 114
config.snmp.deleteUserEntry 114
config.snmp.deleteTargetEntry 115
config.snmp.deleteV3Group 115

config.snmp.sendTestTrap 116
config.snmp.setSNMPv3State 116
config.snmp.setFaMibVersion 117
config.snmp.setState 117
config.snmp.show 118
config.snmp.showAccessTable 119
config.snmp.showTargetTable 121
config.snmp.showUserTable 121
config.snmp.showV3GroupTable 122
config.snmp.showViewTable 123
config.snmp.validateUser 124
config.switch. 125
config.switch.apiState 125
config.switch.banner 126
config.switch.banner.bannerText 126
config.switch.banner.setCLIState 127
config.switch.banner.setWebState 128
config.switch.banner.show 128
config switch blockDupWWN 129
config.switch.domainIDOffset 129
config.switch.domainRSCN 130
config.switch.edTOV 131
config.switch.haMode 131
config.switch.insistDomainId 132
config.switch.interopMode 132
config.switch.islFSPFCost 133
config.switch.ltdFabRSCN 134
config.switch.prefDomainId. 134
config.switch.priority 135
config.switch.raTOV 135
config.switch.rerouteDelay 136
config.switch.RSCNZoneIsolation 137
config.switch.safeZoning 137
config.switch.setipv6 138
config.switch.speed 138
config.switch.show 139
config.switch.webState 141
config.switch.zoneFlexPars 141
config.switch.zoningRSCN 142
config.syslog 142
config.syslog.addServer. 142
config.syslog.deleteServer 143
config.syslog.setLogConfig 143
config.syslog.setState 144
config.syslog.show 144
config.system.contact 145
config.system.date 146
config.system.description 146
config.system.location 147
config.system.name 147
config.system.show 148
config.tunnel.add 149

config.tunnel.delete 149
config.tunnel.edit 150
config.tunnelroute.edit 150
config.tunnel.show 151
config.tunnelroute.add 151
config.tunnelroute.delete 152
config.tunnelroute.show 152
config.zoning 153
config.zoning.activateZoneSet 154
config.zoning.addPortMem 154
config.zoning.addWwnMem 155
config.zoning.addZone 156
config.zoning.clearZone. 157
config.zoning.clearZoneSet 157
config.zoning.deactivateZoneSet 157
config.zoning.deletePortMem 158
config.zoning.deleteWwnMem 159
config.zoning.deleteZone 159
config.zoning.disableSplZoneSet 160
config.zoning.renameZone 160
config.zoning.renameZoneSet 161
config.zoning.replaceZoneSet. 162
config.zoning.setDefZoneState 162
config.zoning.showActive. 163
config.zoning.showPending. 163
config.zoning.showActiveSpl 164
config.zoning.showSplZoneState 165

maint 165
maint.port.beacon 166
maint.port.reset 166
maint.system.beacon 167
maint.system.clearSysError. 167
maint.system.ipl 168
maint.system.resetConfig 168
maint.system.setOnlineState 169

perf. 169
perf.AFD 170
perf.AFD.HDDReport 170
perf.AFD.POMReport 170
perf.AFD.show 171
perf.class2 172
perf.class3 173
perf.clearStats 174
perf.errors. 175
perf.link. 176
perf.openTrunking.backPressure 178
perf.openTrunking.congestionThresh. 178
perf.openTrunking.lowBBCreditThresh. 179
perf.openTrunking.setState. 180
perf.openTrunking.show 180
perf.openTrunking.unresCongestion 182

perf.preferredPath 182
perf.preferredPath.clearPath 183
perf.preferredPath.setPath 184
perf.preferredPath.setState 185
perf.preferredPath.showPath 185
perf.preferredPath.showState 187
perf.slowdrainer.sdreport 187
perf.slowdrainer.show 188
Creating Threshold Alerts 188
perf.thresholdAlerts 191
perf.thresholdAlerts.counter.addAlert 191
perf.thresholdAlerts.counter.addPort 192
perf.thresholdAlerts.counter.removePort 193
perf.thresholdAlerts.counter.setCounter 194
perf.thresholdAlerts.counter.setParams 195
perf.thresholdAlerts.counter.show 196
perf.thresholdAlerts.counter.showStatisticTable 196
perf.thresholdAlerts.deleteAlert 197
perf.thresholdAlerts.setState 198
perf.thresholdAlerts.show 198
perf.thresholdAlerts.throughput.addAlert 200
perf.thresholdAlerts.throughput.addPort 201
perf.thresholdAlerts.throughput.removePort 202
perf.thresholdAlerts.throughput.setUtilType 203
perf.thresholdAlerts.throughput.setUtilPercentage 204
perf.thresholdAlerts.throughput.setParams 204
perf.thresholdAlerts.throughput.show 205
perf.thresholdAlerts.throughput.showUtilTypeTable 206
perf.traffic 207

show 208
show.activeAlias 208
show.all 209
show.auditLog 210
show.epFrameLog.config 211
show.epFrameLog.disableTrigger 212
show.epFrameLog.filterClassFFrames 213
show.epFrameLog.noWrap 213
show.epFrameLog.removeFilterPort 215
show.epFrameLog.setFilterPort 215
show.epFrameLog.setTrigger 216
show.epFrameLog.wrap 217
show.eventLog 218
show.fabric.agshow 219
show.fabric.agshow local 220
show.fabric.agshow remote 220
show.fabric.dcfmtable 221
show.fabricLog.noWrap 222
show.fabricLog.wrap 223
show.fabric.nodes 224
show.fabric.ping 225
show.fabric.principal 226
show.fabric.showRouteTable 226

show.fabric.topology 228
show.fabric.traceRoute 229
show.features 231
show.fencing.policies 232
show.ficonCUPZoning 234
show.ficonMS 234
show.frus 235
show.ip.ethernet 237
show.linkIncidentLog 237
show.loginServer 238
show.nameServer 239
show.nameServerExt 241
show.nameServerFC4Types 242
show.NPIV.config 243
show.openSysMS.config 244
show.openSysMS.platformInfo 245
show.openTrunking.config 246
show.openTrunking.rerouteLog 247
show.port.config 248
show.port.exit 249
show.port.info 251
show.port.nodes 253
show.port.opticData 254
show.port.opticEDD 255
show.port.opticHealth 256
show.port.opticInfo 257
show.port.profile 259
show.port.showPortAddr 261
show.port.status 262
show.preferredPath.showPath 266
show.preferredPath.showState 268
show.security.fabricBinding 268
show.security.log 269
show.security.portBinding 270
show.security.switchAcl 271
show.security.switchBinding 272
show.snmp.accessTable 273
show.snmp.targetTable 274
show.snmp.userTable 276
show.snmp.V3GroupTable 277
show.snmp.viewTable 278
show.snmp.config 279
show.splzoning 280
show.switch 281
show.system 283
show.syslog 284
show.thresholdAlerts.alerts 285
show.thresholdAlerts.log 287
show.zoning 289

Appendix A Error Messages

Appendix B Commands and Corresponding Releases

Index

About This Document

In this chapter

- How this document is organized xv
- Supported hardware and software. xvi
- What's new in this document xvi
- Document conventions xvii
- Additional information xviii
- Getting technical help xix
- Document feedback xx

This publication is part of the documentation suite that supports the following products:

- Sphereon™ 4400, 4500, and 4700 Fabric Switches
- Intrepid® 6064 and 6140 Directors

NOTE
For your convenience, we have retained the legacy McDATA names to avoid any confusion. Please refer to Table for the equivalent Brocade names for the legacy McDATA products.

Brocade names for the legacy McDATA products

Brocade Name	Legacy McDATA Names
Brocade EFCM	EFCM
Brocade M-EOS	E/OS
Brocade M-EOSn	E/OSn
Brocade M6140 Director	Intrepid 6140 (ED-6140
Brocade M4400 Switch	Sphereon 4400
Brocade M4500 Switch	Sphereon 4500
Brocade M4700 Switch	Sphereon 4700
Brocade Mi10K Director	Intrepid 10000 Director (i10k)

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- *Chapter 1, "Introduction"*, provides an introduction and overview of the Command Line Interface.
- *Chapter 2, "CLI Commands"*, describes the CLI commands, including their syntax, purpose, and parameters, as well as examples of their usage and any output that they generate.
- *Appendix A, "Error Messages"* lists and explains error messages that may appear while using the CLI.
- *Appendix B, "Commands and Corresponding Releases"* lists each command in the CLI and the release in which the command was added to the CLI.
- An *"Index"* is also provided.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for 9.9.2, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of M-EOSc:

- Brocade Mi10K Director
- Brocade M6140 Director
- Brocade M4400 Switch
- Brocade M4500 Switch
- Brocade M4700 Switch
- Brocade M3016 Switch
- Brocade M3032 Switch
- Brocade M3216 Switch
- Brocade M3232 Switch
- Brocade M4300 Switch

What's new in this document

The following changes have been made since this document was last released:

- Information that was added:
  - show.fabric.Dcfmtable
  - show.fabric.agshow
  - show.fabric.agshow local
  - show.fabric.agshow remote

For further information about new features and documentation updates for this release, refer to the release notes.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
`code` text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, switchShow. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--option, option	Command options are printed in bold.
–**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, --**show** WWN
|	Boolean. Elements are exclusive. Example: --**show** –**mode** egress | ingress

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on Brocade Connect. See "Brocade resources" on page xviii for instructions on accessing Brocade Connect.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, join Brocade Connect. Go to *http://www.brocadeconnect.com* to register at no cost for a user ID and password.

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

http://www.amazon.com

For additional Brocade documentation, visit the Brocade Web site:

http://www.brocade.com

Release notes are available on the Brocade Connect Web site and are also bundled with the Fabric OS firmware.

Other industry resources

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - data collection

   The procedure for data collection through EFCM Basic:

   1. Log to EFCM Basic
   2. Go to "Maintenance > System Files" node
   3. Save file

   The procedure for data collection through EFCM:

   1. Log to Element Manager
   2. Go to "Maintenance>Data Collection" node
   3. Save file

   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs
2. Switch Serial Number

   The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below.:

   FT00X0054E9

The serial number label is located as follows:

- Brocade M6140, M6064— On the front bottom of chassis
- Brocade M4500, M4700, M4300, M3232, M4400, M3016, M3032—On the rear side of switches

3. World Wide Name (WWN)

   Use the **wwn** command to display the switch WWN.

If you cannot use the **wwn** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1 Introduction

In this chapter

- Command Line Interface overview 1
- Entering Command Line Interface commands 1
- Logging in and logging out 12
- Using the commaDelim command 15
- Commenting scripts 16
- ED-5000 Director 17
- Telnet session 18

Command Line Interface overview

This chapter introduces the Command Line Interface (CLI) and describes the essentials for using the CLI commands.

The Command Line Interface (CLI) is a feature that can be used to manage switches and directors. It provides an alternative to the Graphical User Interface (GUI) and web-based (HTTP) interface products.

The CLI can only be used through a Telnet client session in an out-of-band management environment, using the Ethernet port in the director, switch, or SSH. Any hardware platform that supports the Telnet client software can be used.

The primary purpose of the CLI is to automate management of a large number of switches with the use of scripts. CLI commands can also be entered directly at a command line.

Because CLI is not an interactive interface, no prompts are displayed to guide you through a task. If an interactive interface is needed, use the GUI-based or web-based SAN management applications instead of the CLI.

Entering Command Line Interface commands

The CLI commands can be entered directly at the command line of a terminal or coded in a script.

Note that the output examples shown in the other sections of this publication presume that commaDelim is off. For a description of commadelim, refer to "Using the commaDelim command" on page 15.

NOTE
CLI commands are not case-sensitive.

Documentation conventions

Throughout this publication, periods are used to separate the components of a command name. However, the periods cannot be included when the command is actually entered at the terminal or coded in a script. (For a description of how to enter commands, refer to "Navigation of the CLI command tree" on page 10.)

The periods are automatically generated by the CLI while moving through the CLI Command sequence.

```
Root> config
Config> port
Config.Port>
```

Navigation conventions

Basic command line navigation conventions are supported. Table 1 includes the asynchronous commands that are recognized by the CLI.

TABLE 1 CLI command tree navigation conventions

Character Sequence	Common Name	Action or Description
<CR>	Carriage Return	Pass a completed line to the parser.
<DEL>	Delete	Backspace one character and delete the character.
<NL>	New Line	Pass a completed line to the parser.
<SP>	Space	Used to separate keywords.
#	Pound Sign	Used to designate comments in a script.
?	Question Mark	Provide help information.
"	Quotation Mark	Used to surround a single token.
^A	Control-A	Position the cursor to the start of the line.
^B	Control-B	Position the cursor left one character.
^D	Control-D	Delete the current character.
^E	Control-E	Position the cursor to the end of the line.
^F	Control-F	Position the cursor right one character.
^H	Control-H	Backspace one character and delete the character.
^I	Tab	Complete the current keyword.
^K	Control-K	Delete to the end of the line.
^L	Control-L	Redraw the line.
^N	Control-N	Move down one line in the command history.
^P	Control-P	Move up one line in the command history.
^R	Control-R	Redraw the line.
^U	Control-U	Clear the input and reset the line buffer.
^X	Control-X	Clear the input and reset the line buffer.
<ESC>[A	Up Arrow	Move up one line in the command history.

TABLE 1 CLI command tree navigation conventions (Continued)

Character Sequence	Common Name	Action or Description
<ESC>[B	Down Arrow	Move down one line in the command history.
<ESC>[C	Right Arrow	Position the cursor right one character.
<ESC>[D	Left Arrow	Position the cursor left one character.

Command tree

The command tree of the CLI begins from the root. Table 2 shows the CLI command tree. For description of the commands config, maint, perf, and show, refer to Chapter 2, "CLI Commands".

The following commands are not listed in the command tree, but are globally available and are documented in this chapter.

- login (see "login" on page 13)
- logout (see "logout" on page 14)
- commaDelim (see "Using the commaDelim command" on page 15)

Table 2 shows the command tree hierarchy from the root, reading from left to right.

TABLE 2 CLI command tree

config---------	alias ----------	activatePending
		add
		clearPending
		delete
		replacePending
		setCLIState
		setWebState
		showActive
		showPending
	enterpriseFabMode----	setState
	--	
	features ----------	enterpriseFabMode
		ficonMS
		installKey
		NPIV
		openSysMS
		openTrunking
		show
	fencing----------	addPolicy
		addPort
		deletePolicy
		removePort
		setParams
		setState
		show

TABLE 2 CLI command tree (Continued)

	showTypeTable			
ficonCUPZoning----------	addControlHost			
	deleteControlHost			
	setState			
	show			
ficonMS----------	setMIHPTO			
	setState			
	show			
ip----------	ethernet			
	lineSpeed			
	show			
	v6			
ip----------	setHostCtrlState			
NPIV----------	maxPortIDs			
	setState			
	show			
NSTools----------	clearSnapshot			
	saveSnapshot			
	showSnapDiff			
	showSnapshot			
openSysMS----------	setHostCtrlState			
	setState			
port ----------	blocked			
	fan			
	mode			
	name			
	rxCredits			
	show			
	showCredits			
	showPortAddr			
	speed			
	swapPortByAddr			
	swapPortByNum			
	type			
security----------	authentication--------	interface----------	api----------	outgoing
				sequence
			cli----------	sequence
			eport----------	outgoing
				sequence
			nport----------	outging
				sequence
			osms----------	outgoing
				setKey
			serial----------	enhancedAuth

TABLE 2 CLI command tree (Continued)

			show	
			web----------	sequence
		port----------	override	
			show	
security----------	authentication----------	radius----------	attempts	
			deadtime	
			deleteServer	
			server	
			show	
			timeout	
		switch----------	setSecret	
		user----------	add	
			delete	
			modify	
			passExpTime	
			role	
			show	
security ----------	fabricBinding ----------	activatePending		
		addAttachedMembers		
		addMember		
		clearMemList		
		deactivateFabBind		
		deleteMember		
		replacePending		
		showActive		
		showPending		
	portBinding ----------	bound		
		show		
		wwn		
	ssh----------	resetKeys		
		setRenegotiationMB		
		setState		
		show		
	switchAcl----------	addRange		
		deleteRange		
		setState		
		show		
	switchBinding ---------	addMember		
		deleteMember		
		setState		
		show		

TABLE 2 CLI command tree (Continued)

	ssl ----------	generateKeys
		resetKeys
		setAPIState
		setRengotiationMB
		setWebState
		show
snmp ----------	addAccessEntry	
	addAccessViews	
	addCommunity	
	addTargetParams	
	addUserEntry	
	addV1Target	
	addV2Target	
	addV3Group	
	addV3Target	
	authTraps	
	deleteAccessEntry	
	deleteCommunity	
	deleteTargetEntry	
	deleteUserEntry	
	deleteV3Group	
	sendTestTrap	
	setFaMibVersion	
	setSNMPv3State	
	setState	
	show	
	showAccessTable	
	showTargetTable	
	showUserTable	
	showV3GroupTable	
	showViewTable	
	validateUser	
switch ----------	apiState	
	banner----------	bannerText
		setCLIState
		setWebState
		show
	domainIDOffset	
	domainRSCN	
	edTOV	
	haMode	
	islFSPFCost	
	insistDomainId	
	interopMode	
	ltdFabRSCN	

TABLE 2 CLI command tree (Continued)

	prefDomainId
	priority
	raTOV
	rerouteDelay
	RSCNZoneIsolation
	safeZoning
	setipv6
	speed
	show
	webState
	zoneFlexPars
	zoningRSCN
syslog ----------	addServer
	deleteServer
	setLogConfig
	setState
	show
system ----------	contact
	date
	description
	location
	name
tunnel ----------	add
	delete
	show
tunnelroute ----------	add
	delete
	show
zoning ----------	activateZoneSet
	addPortMem
	addWwnMem
	addZone
	clearZone
	clearZoneSet
	deactivateZoneSet
	deletePortMem
	deleteWwnMem
	deleteZone
	renameZone
	renameZoneSet
	replaceZoneSet
	setDefZoneState
	showPending
	showActive

TABLE 2 CLI command tree (Continued)

maint ---------	port ----------	beacon	
		reset	
	system ----------	beacon	
		clearSysError	
		ipl	
		resetConfig	
		setOnlineState	
perf----------	AFD ----------	HDDReport	
		POMReport	
		Show	
	class2		
	class3		
	clearStats		
	errors		
	link		
	openTrunking ---------	backPressure	
		congestionThresh	
		lowBBCreditThresh	
		setState	
		show	
		unresCongestion	
	preferredPath ---------	clearPath	
		setPath	
		setState	
		showPath	
		showState	
	thresholdAlerts -------	counter ----------	addAlert
			addPort
			removePort
			setCounter
			setParams
			show
			showStatisticTable
		deleteAlert	
		setState	
		show	
		throughput ----------	addAlert
			addPort
			removePort
			setUtilType
			setUtilPercentage
			setParams
			show
			showUtilTypeTable
	traffic		

TABLE 2 CLI command tree (Continued)

show ----------	activeAlias	
	all	
	auditLog	
	epFrameLog----------	config
		disableTrigger
		filterClassFFrames
		noWrap
		removeFilterPort
		setFilterPort
		setTrigger
		wrap
	eventLog	
	fabric----------	nodes
		ping
		principal
		showRouteTable
		topology
		traceroute
	fabricLog----------	noWrap
		wrap
	features	
	fencing----------	policies
	ficonCUPZoning	
	ficonMS	
	frus	
	ip ----------	ethernet
	linkIncidentLog	
	loginServer	
	nameServer	
	nameServerExt	
	nameServerFC4Types	
	NPIV----------	config
	openSysMS----------	config
		platformInfo
	openTrunking ----------	config
		rerouteLog
	port ----------	config
		exit
		info
		nodes
		opticData
		opticEDD
		opticHealth
		opticInfo
		profile

TABLE 2 CLI command tree (Continued)

	showPortAddr
	status
	technology
preferredPath ---------	showPath
	showState
security----------	fabricBinding
	log
	portBinding
	switchAcl
	switchBinding
snmp ----------	accessTable
	config
	targetTable
	userTable
	V3GroupTable
	viewTable
switch	
syslog	
system	
thresholdAlerts-------	alerts
	log
zoning	

With the exception of the zoning commands, all the others are listed in alphabetical order.

The commands can be entered in any order, depending on the results you want. However, the order shown in Table 2 for the zoning commands is a typical order in which the zoning commands are entered.

Note that the order in which commands are entered determines the order in which the show commands display the values. For examples of *show* command output, refer to Chapter 2, "CLI Commands".

Navigation of the CLI command tree

To move from the root through any of the four extended branches, enter the name of the next branch as shown in Table 2.

For example, to use the `config.port.name` command to configure the name for port 4 on the switch, enter the series of commands as follows:

```
Root> config
Config> port
Config.Port> name 4 "Sam's Tape Drive"
```

If you want to set the beaconing state of port 4 using the `enter the maint.port.beacon` command, enter the following series of commands.

```
Config.Port> ..
Config> ..
```

```
Root> maint
Maint> port
Maint.Port> beacon 4 true
```

Note that you must return all the way to the root of the tree to transition to another extended branch. When traversing back to the root, the name of each branch cannot be used. Instead, use the double-dot command (two periods) to move back towards the root. Note that only one double-dot command may be entered at a time.

You can use the `root` command to jump directly to the root of the CLI command tree. The previous example, which shows stepping back to the root with the double-dot command, is simplified as follows:

```
Config.Port> root
Root> maint
Maint> port
Maint.Port> beacon 4 true
```

As an easier and simpler method, you can enter the complete command syntax from the `Root>` prompt each time. For example, to issue the `config.port.name` command and then the `maint.port.beacon` command, enter the following commands.

```
Root> config port name 4 "Sam's Tape Drive"
Root> maint port beacon 4 true
```

While entering the complete command syntax, the prompt stays at the root. The use of complete command syntax is particularly useful when writing scripts.

When coding a script, remember to code the appropriate character sequences, which are described in "Navigation conventions" on page 2.

```
Root> config port name 4 "Sam's Tape Drive"<CR>
Root> maint port beacon 4 true<CR>
```

Limitation on movements

The commands that are entered are recorded in a history log.

The history log has limitations under the following conditions.

- If a command has more than 60 characters, the command runs, but the command is not recorded in the history log, and the position in the tree does not change, as shown in the following example.

```
Root> config zoning addWwnMem TheUltimateZone 10:00:00:00
:C9:22:9B:64
Root>
```

Because the command is not recorded in the history, a subsequent asynchronous command (navigation command) cannot depend on it.

- Whenever the position in the CLI command tree moves to a new branch (for example, from `config` to `maint`, `config` to `config.port`, or `config.port` to `config`), the history log is cleared. In this case, any asynchronous commands (for example, the up-arrow command <ESC>[A or the up-arrow keyboard symbol) cannot move the position back towards the root, as shown in this example.

```
Root> config
```

```
Root.Config> port
Root.Config.Port> <ESC>[A
Root.Config.Port>
```

Parameters

Some command parameters accept character strings that include spaces. Quotation marks are required when a string includes spaces.

```
Config.System> location Building_24_Room_16

Config.System> location "Building 24 Room 16"
```

If spaces are not included in a parameter that accepts a string, the quotation marks are not required around that string.

To include quotation marks in a string, use the escape character (\) before the quotation marks.

```
Config.System> location "Building 24 \"Joe's PlayLab\""
```

A null string can be created by using the quotation marks without any space between them.

```
Config.System> location ""
```

Output

Output from the CLI commands is limited to the standard 80 columns supported by most Telnet interfaces. The output is left-aligned.

Logging in and logging out

The CLI allows a single Telnet client to be connected to the switch. If a Telnet client logs out or is inactive for 15 minutes, the client's access times out and another Telnet client may log in.

The Telnet client (user) must log in every time the director or switch is restarted because the current user's access is lost. Examples of a restart include an initial program load (IPL) and any power-off situation.

Types of users

The CLI supports two user access rights- *administrator* and *operator*.

Administrators can use all the commands described in this publication.

Operators can use only the `perf` and `show` branches of the CLI command tree (for example, the `perf.traffic` and `show.system` commands) with the following exceptions.

- `show.preferredPath`
- `show.security`
- `show.thresholdAlerts`

Operators can also execute the globally available commands (`login`, `logout`, and `commaDelim`).

Passwords and secrets

Some commands require you to enter a password or secret before the command can be executed.

Passwords can be ASCII characters in the range of 32 to 126.

Secrets can be any ASCII character (0-255) and are entered as follows:

- Non-printable and extended ASCII characters can be entered by using a backslash.
- Two hexadecimal characters must follow the backslash.
- All printable ASCII characters can be entered using the keyboard or using its hexadecimal value except for the backslash character. If a backslash is desired as part of the password, its hexadecimal representation must be used.

NOTE
Spaces are valid, but the whole password or secret must be in quotation marks, or you must use the hexadecimal value for the quotation mark. Also, when you log in to CLI, you must use quotation marks around the password again.

The following are examples of valid secrets.

```
simplesecret****
```

This is an example of a secret that does not use any special characters.

```
\40\72\A3\F9\12\13\14\15\16\17\18\19\55\33\87\42
```

This is an example of a 4-character length secret that is configured using the hexadecimal representation.

```
a9p\40\40xx\44\88kutfe\89h
```

This is an example of a 7-character length secret that is composed of a mix of hexadecimal and printable ASCII characters.

Globally available commands

The following commands are available globally to all types of users. In addition, these commands can be entered from any position in the CLI command tree.

login

Syntax

```
login
```

Description

This command allows you to log in with either administrator or operator access rights.

The login command is called automatically by the CLI whenever a new Telnet session is activated or new administrator access rights are configured.

Users are prompted to change the password after logging in with the default password (*password*). However, at the next log in, they are required to change the password if the default password is still being used.

A user name and password can be set by the administrator through the `config.security.authentication.user.add` command or through the `config.security.authentication.user.modify` command.

NOTE
Access rights chosen for the CLI are completely independent of the other product interfaces, for example, SNMP or product interfaces.

Parameters

This command has no parameters.

Command examples

```
login
Username: Administrator
Password: password

login
Username: Operator
Password: password
```

logout

Syntax

```
logout
```

Description

This command logs out the single Telnet client connected to the switch. This command can be entered at any point in the command tree.

Parameters

This command has no parameters.

Command examples

```
Root> logout

Config> logout

Config.Port> logout
```

Using the commaDelim command

Note that the output examples shown in the other sections of this publication presume that commaDelim is off.

commaDelim

Syntax

```
commaDelim enable
```

Purpose

This command displays information in comma-delimited, rather than tabular format. Tabular format is the default.

Description

This command can be entered at any point in the command tree.

Parameter

This command has one parameter:

enable	Specifies the comma-delineated state for output. Valid values are *true* to enable and *false* to disable. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> commaDelim true

Config> commaDelim 1

Config.Port> commaDelim false
```

Output example

Output displayed in commaDelim mode is as follows:

```
Root> show eventLog
Date/Time,Code,Severity,FRU,Event Data,
04/12/01 10:58A,375,Major,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
04/12/01 10:58A,375,Major,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
04/12/01  9:58A,385,Severe,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
04/11/01  7:18P,395,Severe,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
```

Handling CLI errors

The following two types of errors are detected by the CLI:

- An error associated with the interface- For example, a keyword is misspelled or does not exist.

```
Root> confg
Error 234: Invalid Command
```

- An error associated with fabric or switch issues- For example, a parameter error is detected by the switch where port 24 is entered for a switch that supports only 16 ports.

```
Root> config port name 24 "Port 24"
Error 218: Invalid Port Number
```

In either case, the command is ignored. The CLI remains at the same point before the command was entered.

The error messages, including the error number and error description, are listed in Appendix A, “Error Messages”.

Using CLI help

Using the question mark (?) within a command helps obtain information about that command.

- If the question mark is used in place of a command keyword, all the keywords at that level of the CLI command tree appear as follows:

```
Root> config system ?
Command identified
contact           - Set the system contact attribute
date              - Set the system date and time
description       - Set the system description attribute
location          - Set the system location attribute
name              - Set the system name attribute
show              - Display the system configuration
```

- If the question mark is used at the end of a recognized command, any parameters for that command appear as follows:

```
Root> config port name ?
                  - name <portNumber> <portName>
```

- If the question mark is used after one or more characters of a keyword, any keywords at that level of the CLI command tree appear as follows:

```
Root> config s?
security snmp switch system
```

Commenting scripts

Use the pound sign (#) to add comments in a script file. The pound sign must be the first character in the line; the CLI ignores everything after the pound sign in that line. The following lines are valid.

```
Root> #Change port 3 to an E_Port<CR>
Root> config port<CR>
config.port> ##################<CR>
config.port> ## Begin Script ##<CR>
```

```
config.port> ##################<CR>
```

The pound sign cannot be used after any other characters (a command, for example) to start a comment. The following is an invalid script line.

```
Root> maint system beacon true # Turn on beaconing<CR>
```

To correct the previous script line, move the comment either before or after the line with the command.

Both the following examples are valid.

```
Root> # Turn on beaconing<CR>
Root> maint system beacon true<CR>

Root> maint system beacon true<CR>
Root> # Turn on beaconing<CR>
```

NOTE
Limit comments to 200 characters per line. Comments of over 200 characters in length may cause unpredictable system behavior.

ED-5000 Director

A subset of CLI commands described in this publication is available on the ED-5000 Director™.

The list of commands for ED-5000 Director are listed in Table 3. For a description of these commands, refer to Chapter 2, "CLI Commands". Note that the globally available commands described in this chapter (login, logout, and commadelim) can also be used on the ED-5000 Director.

TABLE 3 CLI command tree for the ED-5000 director

config ----------	security ----------	userRights ----------	administrator
			operator
			show
maint ----------	system ----------	resetConfig	
show ----------	ip ----------	ethernet	
	port ----------	config	
		info	
		status	
	switch		
	system		
	zoning		

Telnet session

The CLI can be accessed through a Telnet client session in an out-of-band management environment, using the Ethernet port in the director/switch or Secure Shell (SSH).

Any hardware platform that supports the Telnet client software can be used to enter the CLI commands.

Use the *Configure* option in the GUI-based or web-based interfaces to enable/disable Telnet access. Telnet access is enabled by default. Any changes to the enabled state of the Telnet server are retained through system restarts and power cycles.

Ethernet connection loss

If the Ethernet cable is disconnected from the director or switch during a Telnet session, do one of the following:

- Replace the Ethernet cable before the client connection times out. The Telnet session will continue.
- Wait 15 minutes until the client connection times out; then replace the Ethernet cable and restart the connection.
- If the client connection has already timed out, replace the Ethernet cable. Open a GUI-based or web-based interface SAN-management window. Toggle the enabled state of the CLI, thereby clearing the client connection. Restart the client connection.

  After you have re-established the client connection, verify the completeness and accuracy of your configuration.

Chapter

CLI Commands

2

In this chapter

- Command overview 19
- New and changed commands 19
- config 19
- maint 165
- perf 169
- show 208

Command overview

This chapter describes the Command Line Interface (CLI) commands, including their syntax, purpose, and parameters, as well as examples of their usage and any output that they generate.

The listed commands are arranged in alphabetical order. The commands can be entered in any order, depending on the results desired as per the command line tree.

The various *show* commands are usually entered at the end of a group of other commands to verify configuration changes.

New and changed commands

Changed commands

The following CLI command is changed for this edition of the *Brocade M-EOS Command Line Interface User Manual 9.9.2*:

- "config.security.authentication.RADIUS.server" on page 72

config

The config branch of the CLI command tree contains commands that set parameter values on the switch or director. These values are not temporary (session) values but are retained across power cycles.

The commands in the config branch can only be accessed by a user logging in as administrator. CLI commands are activated on the switch immediately except under certain conditions, which are noted in the command description.

In general, the config naming commands (except for the *config.zoning* commands) use the USASCII character set. All of the characters in this 128-character set (the first 7-bit subset of the ISO-8859-1 Latin-1 character set) are valid. Any exceptions are noted in the specific command descriptions.

Consider the following, when configuring through CLI:

- Two special characters, "" (double quotation marks) and ? (question mark) are ignored.
- Double quotation marks ("") are used to enclose passwords that contain a blank space. For example, "da da". The password "da da" with space is considered only when enclosed by the marks.
- Any character after a question mark (?) is not considered, because the question mark is used as a symbol for help.

config.alias

The alias command on the configuration branch enters the alias configuration branch. All commands under this branch operate on a WWN and its named association. The association is unique to the entire fabric and the associations are shared across the fabric.

All operations on WWNs and their associations are performed on a pending area. You need to explicitly activate changes for them to be saved and distributed across a network.

The pending association, by default, is empty. You must explicitly load the active association list using the `replacePending` command. Operations will resume only after this has been done. You must activate the associations after successful completion of the changes.

This setting is specific to the switch on which you run this command.

In a fabric, only aliases are shared fabric wide. The *setWebState* and *setCliState* setting enables the usage of aliases instead of WWNs only for that particular switch. This command enables the usage of alias or WWN only in the user interfaces. Internally, aliases are replaced with WWNs and all processing takes place using WWNs only.

If the use of alias is enabled in the CLI interface, then the following commands will change such that the alias can be taken as a parameter instead of WWN in the CLI interface.

- fabricbinding.addmember
- fabricbinding.deletemember
- portbinding.addmember
- portbinding.deletemember
- switchbinding.addmember
- switchbinding.deletemember
- zoning.addwwnmember
- zoning.deletewwnmember
- security.authentication.user.add
- ficoncupzoning.addControlhost
- ficoncupzoning.deletecontrolhost
- show.security.portbinding
- show.port.profile
- show.port.info

- show.fabric.ping

In addition, for all the commands that display a WWN, an alias is displayed in its place if there is one configured.

config.alias.activatePending

Syntax

```
activatePending
```

Description

This command saves the pending alias association list to memory and distributes it in the fabric. This should be the final command executed after configuring all the desired WWN to alias association in the pending area.

Parameters

This command has no parameters.

Command example

```
Root> config alias activatePending
```

config.alias.add

Syntax

```
add wwn alias
```

Description

This command adds the association that exists between a WWN and its alias from the pending alias database. This command can be run only after copying the active association list into the pending list using the `replacePending` command. The parameter should be any one member of the association – either the WWN or the alias.

Parameters

This command has two parameters:

wwn	The WWN to associate with the alias. WWNs cannot be all zeros.
alias	An alias string of up to 24 characters. Embedded blanks are allowed. The first character cannot be blank and trailing blanks are removed. An alias cannot be a WWN.

Command example

```
Root> config alias add 1:1:1:1:1:1:1:1 AliasName
```

config.alias.clearPending

Syntax

```
clearPending
```

Description

This command clears the user-modified changes in the pending alias association list.

Parameters

This command has no parameters.

Command example

```
Root> config alias clearPending
```

config.alias.delete

Syntax

```
delete parameter
```

Description

This command removes the association that exists between a WWN and its alias from the pending alias database. This command can be run only after copying the active association list into the pending list using the `replacePending` command. The parameter should be any one member of the association – either the WWN or the alias.

Parameters

This command has one parameter.

parameter	The WWN or alias.

Command example

```
Root> config alias delete 11:22:33:44:55:66:77:88
or
Root> config alias delete AliasName
```

config.alias.replacePending

Syntax

```
replacePending
```

Description

This command copies the list of the active alias associations to the pending alias association list.

Parameters

This command has no parameters.

Command example

```
Root> config alias replacePending
```

config.alias.setCLIState

Syntax

```
setCLIState state
```

Description

This command configures the usage of aliases in place of WWNs in the CLI interface.

Parameters

This command has one parameter.

state	The enabled/disabled state for displaying aliases in the CLI interface. Valid values are *enable* and *disable*. Boolean *1* and *0* values may also be substituted.

Command example

```
Root> config alias setCLIState 1
or
Root> config alias setCLIState disable
```

config.alias.setWebState

Syntax

```
setWebState state
```

Description

This command configures the state for displaying aliases in place of WWNs in the web interface.

Parameters

This command has one parameter:

state	The enabled/disabled state for displaying Aliases in the Web interface. Valid values are *enable* and *disable*. Boolean *1* and *0* values may also be substituted.

Command example

```
Root> config alias setWebState 1
or
Root> config alias setWebState disable
```

config.alias.showActive

Syntax

```
showActive
```

Description

This command displays all the alias entries that are available in the active alias database.

Parameters

This command has no parameters.

Output

This command displays the currently associated WWNs and their aliases that are in the active association list. Also, it displays the current associations count and possible total associations count.

Output example

```
Config.Alias> showActive
CLI Alias enabled state:        Enabled
Web Alias enabled state:        Disabled
Total associations possible:    250
Current associations:           4
WWN                     Alias
----------------------  ----------------
11:22:33:44:55:66:77:11  FirstSwitch
22:22:33:44:55:66:77:12  SecondSwitch
33:22:33:44:55:66:77:13  Row2Rack1Lower
44:22:33:44:55:66:77:11  Row2Rack1Upper
```

config.alias.showPending

Syntax

```
showPending
```

Description

This command displays the alias entries that are available in the pending alias database.

Parameters

This command has no parameters.

Output

This command displays the currently associated WWNs and their aliases that are in the active association list. Also, it displays the current associations count and possible total associations count.

Output example

```
Config.Alias> showPending
CLI Alias enabled state:        Disabled
Web Alias enabled state:        Disabled
Total Associations Possible:    250
Current Associations:           4
WWN                     Alias
----------------------  -----------------
11:22:33:44:55:66:77:11  FirstSwitch
22:22:33:44:55:66:77:12  SecondSwitch
33:22:33:44:55:66:77:13  Row2Rack1Lower
44:22:33:44:55:66:77:11  Row2Rack1Upper
```

config.enterpriseFabMode.setState

Syntax

```
setState enterpriseFabModeState
```

Description

This command sets the Enterprise Fabric Mode state for the fabric. The SANtegrity™ feature key must be installed to activate the Enterprise Fabric Mode state.

NOTE
The command "config.features.enterpriseFabMode" on page 26 has functionality that is identical to this command.

Parameters

This command has one parameter:

enterpriseFabModeState	The active/inactive state of enterpriseFabMode. Valid values are *activate* and *deactivate*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config enterpriseFabMode setState 1
```

NOTE
Open Trunking should be disabled before activating Enterprise Fabric Mode.

config.features.enterpriseFabMode

Syntax

```
enterpriseFabMode enterpriseFabModeState
```

Description

This command sets the Enterprise Fabric Mode state for the fabric. The SANtegrity™ feature key must be installed to activate the Enterprise Fabric Mode state.

Parameters

This command has one parameter:

enterpriseFabModeState	The active/inactive state of enterpriseFabMode. Valid values are *activate* and *deactivate*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config features enterpriseFabMode 1
```

NOTE
The command “config.enterpriseFabMode.setState” on page 25 has functionality that is identical to this command

config.features.ficonMS

Syntax

```
ficonMS ficonMSState
```

Description

This command enables or disables the FICON Management Server. The FICON Management Server feature key must be installed in order to enable the FICON Management Server State.

Sphereon 4300 and Sphereon 4500 switches do not accept this command. This command is displayed on Sphereon 3016 and 3216 switches only if the feature key is installed.

NOTE
If the FICON Management Server is enabled, the default management style is the FICON Management Style. The Open Systems Management Style cannot be used.

Parameters

This command has one parameter:

ficonMSState	The enabled/disabled state of the FICON Management Server. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config features ficonMS 1
```

NOTE
The command "config.ficonMS.setState" on page 40 has functionality that is identical to this command.

config.features.installKey

Syntax

```
installKey featureKey
```

Description

This command installs a feature set based on a provided feature key. The switch can be either offline or online when this command is executed.

NOTE
If any currently installed features are being removed by the new feature key, the switch must be offline when the command is given.

Parameters

This command has one parameter:

featureKey	The key you have received to enable an optional software feature on a specific product. A feature key is a string of case-sensitive, alphanumeric ASCII characters. The number of characters may vary in the format; however, the key must be entered exactly, including the hyphens. An example of a feature key format is XxXx-XXxX-xxXX-xX.

Command example

```
Root> config features installKey AaBb-CCdD-eeFF-gH
```

config.features.NPIV

Syntax

```
setState NPIVState
```

Description

This command enables or disables the NPIV feature. The NPIV feature key must be installed in order to enable this feature.

Parameters

This command has one parameter.

NPIVState	The enabled/disabled state of NPIV. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config features NPIV enable
```

NOTE
The command "config.NPIV.setState" on page 46 has functionality that is identical to this command.

config.features.openSysMS

Syntax

```
openSysMS openSysMSState
```

Description

This command enables or disables Open Systems Management Server (OSMS). OSMS is a feature that allows host control and inband management of the switch or director through a management application that resides on an Open-Systems Interconnection (OSI) device.

Parameters

This command has one parameter:

osmsState	The enabled/disabled state of Open Systems Management Server. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config features openSysMS 1
```

NOTE
The command "config.openSysMS.setState" on page 50 has functionality that is identical to this command.

config.features.openTrunking

Syntax

```
openTrunking openTrunkingState
```

Description

This command enables or disables the OpenTrunking feature. The OpenTrunking feature key must be installed in order to enable open trunking.

Parameters

This command has one parameter:

openTrunkingState	The enabled/disabled state of the OpenTrunking feature. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config features openTrunking 1
```

NOTE
The command "perf.openTrunking.setState" on page 180 has functionality that is identical to this command.

config.features.show

Syntax

```
show
```

Description

This command shows the product feature information configured for this director or switch.

Parameters

This command has no parameters.

Command example

```
Root> config features show
```

Output

The product feature data is displayed as a table that includes the following properties.

Installed Feature Set	The feature set installed using a feature key. Only installed keys are displayed.
Feature	Individual features within each set. In many cases, there is only one feature within each feature set.
State	The state of the individual feature. Fabric-wide features are displayed as *Active/Inactive*. Features related to the switch are displayed as *Enabled/Disabled*.
Exp	The remaining evaluation time in days for the trial feature.

Output example

The output from the *config.features.show* command displays as follows.

```
Installed Feature Set           Feature                         State     Exp
-----------------------------  ------------------------------  --------  -----
Security Package
  SANtegrity Binding            Switch Binding                  Enabled
  SANtegrity Binding            Fabric Binding                  Active
  SANtegrity Binding            Enterprise Fabrics              Active
  SANtegrity Authentication     SANtegrity Authentication       Enabled

FICON Cascading Bundle
  FICON Management Server       FICON Management Server         Enabled
  FICON CUP Zoning              FICON CUP Zoning                Active
  OpenTrunking                  OpenTrunking                    Active
```

NOTE
The command “show.features” on page 231 has functionality that is identical to this command.

config.fencing

The fencing command on the configuration branch enters the fencing configuration branch. All commands under this branch operate on the port fencing feature.

config.fencing.addPolicy

Syntax

```
addPolicy name
```

Description

This command configures a new fencing policy and assigns it a name. The new policy is assigned default settings, which must be changed before the policy is activated.

Refer to the command "config.fencing.setParams" on page 34 for default settings.

Parameters

This command has one parameter.

name	The name of the new fencing policy. This name can consist of any printable USASCII characters up to a maximum length of 63 characters. This parameter is case-sensitive.

Command example

```
Root> config fencing addPolicy Policy2
```

NOTE
The maximum number of policies supported is 14.

config.fencing.addPort

Syntax

```
addPort name portNumber
```

Description

This command adds a port to the specified fencing policy.

Parameters

This command has two parameters:

name	The name of the fencing policy.
portNumber	The port number to add to the fencing policy, or *all*, which adds all of the individual ports to the fencing policy. Valid values for the port number are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

NOTE
A range of ports is not accepted as a valid input to this command (e.g., “0-29” is not acceptable).

The port values can also be substituted with one of the following keywords that removes all the ports from the alert, and then uses a specific type of port instead of individual port numbers.

Valid values are:

- *eport* – This adds all active E_ports.
- *fport* – This adds all active F_ports.
- *flport* – This adds all active F_Ports and FL_ports (This applies to Sphereon 4400, Sphereon 4300, Sphereon 4500 and Sphereon 4700 switches).

NOTE
A fencing policy can contain either port types or individual port numbers only.

Command example

```
Root> config fencing addPort 24
Root> config fencing addPort eport
```

config.fencing.deletePolicy

Syntax

```
deletePolicy  name
```

Description

This command deletes the specified fencing policy. Only disabled fencing policies can be deleted.

Parameters

This command has one parameter:

name	The name of the fencing policy. You can also enter *all* for this argument. This deletes all of the configured fencing policies.

Command example

```
Root> config fencing deletePolicy Policy1
```

config.fencing.removePort

Syntax

```
removePort  name  portNumber
```

Description

This command removes a port from the specified fencing policy.

Parameters

This command has two parameters:

name	The name of the fencing policy.
portNumber	The port number to remove from the fencing policy, or *all*, which removes all of the individual ports from the fencing policy. 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> config fencing removePort 24
```

config.fencing.setParams

Syntax

```
setParams name typeNumber limit period
```

Description

This command sets the type, limit, and period values for the specified fencing policy.

Parameters

This command has four parameters:

name	The name of the fencing policy.
typeNumber	A number that corresponds to an entry in the table shown below.
limit	The count of fencing violations that must occur within the specified period in order for a port to be automatically disabled. Acceptable values are in the range of 1-255. You may also enter *default* for this argument, which sets the default limit value for this fencing policy type.
period	The number of seconds in which the violation count must equal or exceed the threshold limit in order for a port to be fenced. You may also enter *default* for this argument, which sets the default period for this fencing policy type.

NOTE
The interval value is a fixed length amount of time. This interval is not a rolling window interval.

Table 2-1

Type Number	Policy Type	Limit Value Range	Period Value Range
1	Protocol Errors	5	300 seconds
1	Protocol Errors	1 - 255	60 - 1800 seconds

Command example

If ports 0, 1, or 2 have more than five protocol errors on a single port within a period of 30 minutes, disable the offending port.

Where:

Port list	= 0, 1, 2
Fencing Type	= Protocol Errors
Limit	= 5
Period	= 1800 seconds

Command example

```
Root> Config fencing setParams abc 1 5 300
```

config.fencing.setState

Syntax

```
setState name enabledState
```

Description

This command enables or disables the specified fencing policy. A policy cannot be activated if it contains ports that are already controlled by a different fencing policy of the same type.

Parameters

This command has two parameters:

name	The name of the fencing policy.
enabledState	The enabled/disabled state of the specified fencing policy. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config fencing setState enable
```

config.fencing.show

Syntax

```
show name
```

Description

This command displays the settings for fencing policies.

Parameters

This command has one optional parameter:

name	The name of the fencing policy.

When no parameters are specified, the command displays the name, type, and state of all policies. If the optional parameter is specified, it displays all the information about the policy.

NOTE
If the *name* parameter is not supplied, then only 50 characters of the policy name are displayed. In such cases, enable the Comma Delimited Mode to view the full name.

Command example

```
Root> config fencing show
Root> config fencing show Policy_1
```

Output

If you do not specify the *name* parameter, then the output shows the following information:

Name	The name of the policy. This is concatenated to 50 characters in the summary display. You can view the policy full name in the comma delim mode.
Ports	The ports to which the fencing policy is applied.
Type	The type of the fencing policy.
Limit	The number of offenses that are allowed before a port is disabled.
Period	The amount of time that *limit of number of offenses* must exceed before a port is fenced.
State	The enabled state of the fencing policy.

Output example

The output from the *config.fencing.show* command displays as follows:

```
Name                           Type             State
-------------------------------------------------------
Default Protocol Error Policy  Protocol Error   Disabled
Policy_1                       Protocol Error   Disabled
```

The output from the *config.fencing.show Policy_1* command displays as follows:

```
Name:         Policy_1
Ports:        E ports
Type:         Protocol Error
Limit:        5
Period:       300 seconds
```

```
State:        Disabled
```

config.fencing.showTypeTable

Syntax

```
showTypeTable
```

Description

This command displays the table of different fencing types that can be assigned to a policy. This table is used for reference only.

Parameters

This command has no parameters.

Command example

```
Root> config fencing showTypeTable
```

Output example

The output from the *config.fencing.showTypeTable* command displays as follows:

```
Number     Fencing Policy Types
--------------------------------
1          Protocol Error
2          Link Level Hot I/O
3          Security Violationss
```

config.ficonCUPZoning

The ficonCUPZoning commands add functionality to the FICON CUP Zoning branch by adding the ability to configure the Host Control List for the FCZ feature. The commands are shown only when both the FMS and FCZ feature key are installed.

config.ficonCUPZoning.addControlHost

Syntax

```
addControlHost  hostNodeWwn
```

Description

This command adds a control host to the Control Host List used to determine the FICON hosts capable of viewing all ports. This list overrides the FCZ port visibility mask. The maximum entries in this list is 8.

Parameters

This command has one parameter:

hostNodeWwn	The node World Wide Name (WWN) of the desired control host, entered in colon-delimited notation (e.g., 01:02:03:04:05:06:07:08).

Command example

```
Root> config ficonCUPZoning addControlHost 01:02:03:04: 05:06:07:08
```

config.ficonCUPZoning.deleteControlHost

Syntax

```
deleteControlHost  hostNodeWwn
```

Description

This command removes one or all control hosts from the Control Host List used to determine the FICON hosts capable of viewing all ports. This list overrides the FCZ port visibility mask.

Parameters

This command has one parameter:

hostNodeWwn	The node WWN of the desired control host, entered in colon-delimited notation (e.g., 01:02:03:04:05:06:07:08). You can also enter *all* to remove the entire list, if no attached hosts have supervisory privileges.

Command example

```
Root> config ficonCUPZoning deleteControlHost all
```

config.ficonCUPZoning.setState

Syntax

```
setState ficonCUPZoningState
```

Description

This command enables or disables FICON CUP Zoning. The FICON Management Server feature key must be installed in order to enable the FICON CUP Zoning State.

Sphereon 4300 and Sphereon 4500 switches do not accept this command.

NOTE
If the FICON Management Server is enabled, the default management style is the FICON Management Style. The Open Systems Management Style cannot be used.

Parameters

This command has one parameter.

ficonCUPZoningState	The enabled/disabled state of the FICON Management Server. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config ficonCUPZoning setState 1
```

config.ficonCUPZoning.show

Syntax

```
show
```

Description

This command displays the contents of the host control list and the enabled state of FICON CUP Zoning.

Parameters

This command has no parameters.

Command example

```
Root> config ficonCUPZoning show
```

Output

The data is displayed as a table that includes the following information:

FICON CUP Zoning State	The enabled state of the FICON CUP Zoning feature.
Host Control List	List of 0-8 control hosts, displays “empty” for control host list with no members.

Output example

The output from the *config ficonCUPZoning show* command displays as follows:

```
FICON CUP Zoning State:     Enabled

Host Control List
-----------------------
01:02:03:04:05:06:07:08
09:0A:0B:0C:0D:0E:0F:00
```

NOTE
The command "show.ficonCUPZoning" on page 234 has functionality that is identical to this command.

config.ficonMS.setMIHPTO

Syntax

```
setMIHPTO timeout
```

Description

This command sets the FICON MS MIHPTO value in seconds.

Parameters

This command has one parameter:

timeout	The length of time, in seconds, after which the MIHPTO timer expires. Valid values are 15, 30, 45, 60, 120, 180, 240, 300, 360, 420, 480, 540, and 600. The default value is 180 seconds.

Command example

```
Root> config ficonms setMIHPTO 180
```

config.ficonMS.setState

Syntax

```
setState ficonMSState
```

Description

This command enables or disables the FICON Management Server. The FICON Management Server feature key must be installed in order to enable the FICON Management Server State.

The Sphereon 4300 and Sphereon 4500 switches do not accept this command. This command is displayed on a Sphereon 3016 only if the feature key is installed.

NOTE
If the FICON Management Server is enabled, the default management style is the FICON Management Style. The Open Systems Management Style cannot be used.

Parameters

This command has one parameter:

ficonMSState	The enabled/disabled state of FICON Management Server. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config ficonMS setState 1
```

NOTE
The command "config.features.ficonMS" on page 27 has functionality that is identical to this command.

config.ficonMS.show

Syntax

```
show
```

Description

This command shows the FICON MS settings.

Parameters

This command has no parameters.

Command example

```
Root> config ficonMS show
```

Output

The data is displayed as a table that includes the following information:

Ficon MS State	The state of the FICON MS feature.
Ficon MIHPTO	The FICON MIHPTO value in seconds.

Output example

The output from the *config.ficonMS.show* command displays as follows:

```
Ficon MS State: Disabled
Ficon MIHPTO (seconds):   180
```

config.ip.ethernet

Syntax

```
ethernet ipAddress gatewayAddress subnetMask
```

Description

This command sets the Ethernet network settings. If the IP address is reconfigured, the Telnet client must be reconnected to the new IP address. A new login will be requested.

NOTE
The Telnet connection can be lost when these Ethernet network settings are changed.

Parameters

This command has three parameters:

ipAddress	The new IP address for the director or switch. The address must be entered in dotted decimal format (for example, 10.0.0.0).
gatewayAddress	The new gateway address for the Ethernet interface. The address must be entered in dotted decimal format (for example, 0.0.0.0).
subnetMask	The new subnet mask for the Ethernet interface. The address must be entered in dotted decimal format (for example, 255.0.0.0).

Command example

```
Root> config ip ethernet 10.0.0.0 0.0.0.0 255.0.0.0
```

config.ip.lineSpeed

Syntax

```
lineSpeed speed duplex
```

Description

This command sets the Ethernet line speed.

Parameters

This command has two parameters. One of the parameters is optional depending on the combination.

speed	The line speed. Options are *auto*, *10,* or *100.* If *auto* is entered then the optional *duplex* should not be entered.
duplex	The duplex mode for the connection. Options are *full* or *half*.

Command example

```
Root> config ip lineSpeed 10 half
```

config.ip.show

Syntax

```
show
```

Description

This command shows the LAN configuration.

Parameters

This command has no parameters.

Command example

```
Root> config ip show

IPV6 Address/Prefix:     2602::175/64
IPV6 Gateway Address:    2602::1
IPV6 State:              Enabled
IPV4 Address:            172.26.26.175
IPV4 Gateway Address:    172.26.26.1
Subnet Mask:             255.255.255.0
Line Speed:              100Mbps Full-duplex
```

Output

The LAN configuration data is displayed as a table that includes the following properties.

IP Address	The IP address.(either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format))
Gateway Address	The gateway address.
Subnet Mask	The subnet mask.

Output example

The output from the *config.ip.show* command displays as follows:

```
IP Address:        10.0.0.0
Gateway Address:   0.0.0.0
Subnet Mask:       255.0.0.0
```

config.ip.v6

Syntax

```
IPv6 <ipv6Address> <ipv6gatewayAddress> <prefix>
```

Description

This command sets the Ethernet network settings. If the IPv6 address is reconfigured, the telnet client must be reconnected to the new IPv6 address. A new login will be requested.

Parameters

.

ipv6Address	The new IPV6 Address for the product. The address must be entered in hexadecimal colon based format (eg., 2001:: 112:221:FFA)
ipv6gatewayAddress	The new gateway address for the Ethernet interface. The address must be entered in hexadecimal colon based format (E.g., A34::20)
Prefix	validate the integer value from 4-128

Command example

```
Root> Root> config ip v6   2002::122 1001::11 125
```

config.NPIV

N_Port ID Virtualization (NPIV) provides an FC facility for sharing a single physical N_Port among multiple N_Port IDs, thereby allowing multiple initiators, each with its own N_Port ID, to share the N_Port.

You can configure the number of allowed NPIV logins for a given port and enable or disable the feature.

Valid values for the *Login Limit* are 1 to 256. The default value is set to 128. When the feature is enabled, the NPIV number cannot be lowered if the NPIV devices have been logged in already.

NOTE
From 9.6 release NPIV is declared as a free feature and hence the Product Feature Enablement key is no more required to enable NPIV feature in the switch.

config.NPIV.maxPortIDs

Syntax

```
maxPortIDs  portNumber  maxIDs
```

Description

This command configures the maximum number of NPIV logins that are allowed on the specified port.

Parameters

This command has two parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 all - applies the maxIDs parameter value to every port on the product.
maxIDs	The maximum number of NPIV logins allowed on the specified port.Valid values are in the range 1–256.

Command example

```
Root> config NPIV maxPortIDs 128

Root> config NPIV portNumber 60
```

config NPIV setALPAREstate

Syntax

```
setALPAREstate <ALPAREASSIGNState>
```

Description

This command sets the enabled state of the ALPAREASSIGN feature.

Parameters

This command has one parameter:

ALPAREASSIGNState	The enable\disable the state of the feature.

Command example

```
Root> Config NPIV setALPAREstate 1
```

config.NPIV.setState

Syntax

```
setState NPIVState
```

Description

This command sets the enabled state of the NPIV feature.

Parameters

This command has one parameter:

NPIVState	The enabled/disabled state of the feature. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config NPIV setState enable
```

config.NPIV.show

Syntax

```
show
```

Description

This command displays the current NPIV configuration for all ports.

Parameters

This command has no parameters.

Command example

```
Root> config NPIV show
```

Output

This command displays the following NPIV configuration data:

NPIV state	The current enabled/disabled state of the NPIV feature.
Max Allowed	The NPIV Login Table. A table mapping each port number on the switch to a corresponding max number of NPIV logins setting.

Output example

The output from the *config.NPIV.show* command displays as follows:

```
NPIV state:Enabled
Port       Max Allowed NPIV Logins
---------------------------
1       10
2       10
3       10
4       0
5       0
6       130
...
```

NOTE
The command "show.NPIV.config" on page 243 has functionality that is the same as this command.

config.NSTools

The NSTools command on the configuration branch enters the NSTools configuration branch. All commands under this branch operate on the name server snapshot database.

config.NSTools.clearSnapshot

Syntax

```
clearSnapshot
```

Description

This command clears the name server database entries from the snapshot database that was saved.

Refer to *config.NSTools.saveSnapshot* for saving the snapshot.

Parameters

This command has no parameters.

Command example

```
Root> config NSTools clearSnapshot
```

config.NSTools.saveSnapshot

Syntax

```
saveSnapshot
```

Description

This command captures a list of FC IDs in the local name server database with the timestamp of when the list was created.

Parameters

This command has no parameters.

Command example

```
Root> config NSTools saveSnapshot
```

Output example

The output from the *config.NSTools.saveSnapshot* command displays as follows:

```
config.NSTools> saveSnapshot
Saving snapshot of the NameServer Database ...
Snapshot Time:    09/15/2005 19:25:43
```

config.NSTools.showSnapDiff

Syntax

```
showSnapDiff
```

Description

This command displays a list of FC IDs of nodes that have logged in or logged out from the name server since the last snapshot was taken.

Parameters

This command has no parameters.

Command example

```
Root> config NSTools showSnapDiff
```

Output

The following properties are displayed:

Snapshot Time	The time at which the name server snapshot was taken.
Current Time	The current date and time.
Additional NS Entries	A list of FC IDs of nodes that logged into the name server after the snapshot was taken.
Missing NS Entries	A list of FC IDs of nodes that are not logged into the name server but were logged into the name server at the time of snapshot was taken.

Output example

The output from the *config.NSTools.showSnapDiff* command displays as follows:

```
config.NSTools> showSnapDiff
Snapshot Time:    02/27/2006 22:35:41
Current Time:     02/27/2006 22:36:04

Missing NS Entries:
-------------------
610513

Additional NS Entries:
----------------------
610413
610713
```

config.NSTools.showSnapshot

Syntax

```
showSnapshot
```

Description

This command displays the list of FC IDs saved in the snapshot.

Parameters

This command has no parameters.

Command example

```
Root> config NSTools showSnapshot
```

Output example

The output from the *config.NSTools.showSnapshot* command displays as follows:

```
Config.NSTools> showsnapshot
Snapshot Time:    02/27/2006 22:35:41

Saved NS Entries
----------------
690BDC
690BE0
690BE1
690BE2
690BE4
690BE8
```

config.openSysMS.setHostCtrlState

Syntax

```
setHostCtrlState HostContrlState
```

Description

This command enables or disables Open Systems Management Server (OSMS) Host Control.

Parameters

This command has one parameter:

HostContrlState	The enabled/disabled state of OSMS. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config openSysMS setHostCtrlState enable
```

config.openSysMS.setState

Syntax

```
setState osmsState
```

Description

This command enables or disables the Open Systems Management Server (OSMS) feature.

OSMS is a feature that allows host control and in-band management of the switch or director through a management application that resides on an Open-Systems Interconnection (OSI) device.

Parameters

This command has one parameter.

osmsState	The enabled/disabled state of the Open Systems Management Server. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config openSysMS setState 1
```

NOTE
The command "config.features.openSysMS" on page 28 has functionality that is identical to this command.

config.port.blocked

Syntax

```
blocked portNumber blockedState
```

Description

This command sets the blocked state for a port.

Parameters

This command has two required parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
blockedState	The blocked state for the port. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> config port blocked 4 false

Root> config port blocked 4 0
```

config.port.fan

Syntax

```
fan portNumber fanState
```

Description

This command sets the Fabric Address Notification (FAN) state for a port (Sphereon 4300 and Sphereon 4500 switches only). This configuration can be applied to any port regardless of its current configuration. The FAN value is applied at the time the port is configured and operated in a loop.

Parameters

This command has two required parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3232 0–31 for the Sphereon 4700
fanState	The FAN state for the port. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config port fan 4 1
```

config.port.name

Syntax

```
name portNumber portName
```

Description

This command sets the name for a port.

Parameters

This command has two required parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portName	The name for the port. The port name must not exceed 24 characters in length.

Command example

```
Root> config port name 4 Sam's tape drive
```

config.port.rxCredits

Syntax

```
rxCredits PortNumber RxCredits
```

Description

This command sets the number of initial BB_Credits for a given port. The number of credits assigned must fall between the minimum and maximum allowed values for the port.

Parameters

This command has two required parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
numBBCredits	The number of Rx BB_Credits to assign the specified port. For the Sphereon 4300 and Sphereon 4500 the RxCredits per port must be between 2 and 12. The total number of Rx Credits assigned across all ports must not exceed the maximum pool size of 150. For the Intrepid family, the RxCredits per FPM/UPM port must be between 1 and 60. The RxCredits per XPM port must be between 4 and 400. There is no pool limitation.

Command example

```
Root> config port rxCredits 8 40
```

config.port.show

Syntax

```
show portNumber
```

Description

This command displays the current configuration for the specified port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–12 for the Sphereon 4300 0–15 for the Sphereon 3016 0–16 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–32 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> config port show 4
```

Output

This command output displays as a table that includes the following properties:

Port Number	The port number.
Name	The configured port name.
Blocked	The blocked state. Valid values are *true* and *false*.
Blocked Reason	The reason for port being blocked. Valid values are *'Blocked temporarily, Internal'*, '*Blocked by user*', '*Blocked by hardware type change*', *'Blocked by port fencing*'.
FAN	The Fabric Address Notification (FAN) state. Valid values are *enabled* and *disabled*. (Sphereon 4300 and Sphereon 4500 switches only.)
Type	The port type. Valid values are: *F Port* *E Port* *G Port* *Fx Port (Sphereon 4300, Sphereon 4400, Sphereon 4500, and Sphereon 4700 only)* *Gx Port (Sphereon 4300, Sphereon 4400, Sphereon 4500, and Sphereon 4700 only)*
Speed	The configured port speed. Valid values are: *1G – 1 Gb/sec* *2G – 2 Gb/sec* *4G – 4 Gb/sec (Sphereon 4400 and Sphereon 4700 only)* *10G – 10 Gb/sec (XPM only)* *Neg - Negotiate* *4G Burst – 4 Gb/sec Burst (QPM only)* *4G Sust – 4 Gb/sec Sustained (QPM only)* *Neg Sust – Negotiate Sustained (QPM only)* *Neg 2G Max – Negotiate 2 Gb/sec Maximum (QPM only)* *Neg B 4G Max – Negotiate Burst 4 Gb/sec Maximum (QPM only)*
Rx BB_Credits	The number of configured Rx BB_Credits.

Output example

The output from the *config.port.show* command displays as follows:

```
Port Number:          4
Name:                 Sam's tape drive
Blocked:              false
Blocked Reason:
Type:                 F Port
Speed:                4G Burst
Rx BB_Credits:        12
```

config.port.showPortAddr

Syntax

```
showPortAddr
```

Description

This command displays the port address configuration for all ports.

NOTE
The command "show.port.showPortAddr" on page 261 has similar functionality.

Parameters

This command has no parameters.

Command example

```
Root> config port showPortAddr
```

Output

The port configuration is shown as a table of properties. The following properties are displayed:

Port	The port number.
Original Addr	The original port address of the port.
Current Addr	The current port address of the port.
Swapped Port Num	If the port is swapped with another port, it displays the port number of the port it is swapped with.

Output example

```
Port   Original Addr     Current Addr  SwappedPort Num
----   -------------     ------------  ---------------
0      4                 4
1      5                 5
2      6                 7             3
3      7                 6             2
4      8                 8
5      9                 9
6      a                 a
7      b                 b
8      c                 c
...
```

config.port.showCredits

Syntax

```
showCredits
```

Description

This command shows the BB_Credit Pool information.

Parameters

This command has no parameters.

Command example

```
Root> config port showCredits
```

Output

This command displays the BB_Credit data:

Pool	The BB_Credit pool. Possible values: Sphereon 4300 – Pool 0 Sphereon 4400 – Pool 0 Sphereon 4500 – Pool 0 Sphereon 4700 – Pool 0 and Pool 1
Total	The total number of BB_Credits that this pool contains.
Allocated	The number of BB_Credits that are currently allocated to ports.
Available	The number of BB_Credits that are currently available to allocate to ports.
Ports	A list of port numbers that belong to the pool.

Output example

```
Config.Port> showCredits
Pool    Total  Allocated  Available  Ports
------  -----  ---------  ---------  -----
Pool 1  252    190        62         0-3,8-11,16-19,24-27
Pool 2  252    80         172        4-7,12-15,20-23,28-31
```

or

```
Config.Port> showCredits
Pool    Total  Allocated  Available  Ports
------  -----  ---------  ---------  -----
Pool 1  150    100        50         0-23
```

config.port.speed

Syntax

```
speed portNumber portSpeed
```

Description

This command sets the speed for a port.

This command is available always, but the CLI responds with an error if the hardware supports only one link speed. To change a port speed to 2 Gbps, the switch speed must be configured to 2 Gbps.

NOTE
Port speed changes temporarily disrupt port data transfers.

Parameters

This command has two required parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–16 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–32 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portSpeed	The speed of the port. Valid values are: *1g* *2g* *4g* *Negotiate* *4gSustained* *4gBurst* *negotiateSustained* *negotiateBurst4gMax* negotiate2gMax Note: *4gBurst* and *negotiateBurst4gMax* are applied only to F_port type on QPM cards. To configure to these port speed, you need to first set the port to F_port.

Command examples

```
Root> config port speed 4 2g

Root> config port speed 6 negotiateBurst4gMax
```

config.port.swapPortByAddr

Syntax

```
swapPortByAddr  portAddr1 portAddr2
```

Description

This command swaps two ports given the port addresses. The ports must be offline to perform this operation.

Parameters

This command has two required parameters:

portAddr1	The port address, in hexidecimal format, of the desired port to be swapped.
portAddr2	The port address, in hexidecimal format, of the desired port to be swapped.

Command example

```
Root> config port swapPortByAddr 1e 1f
```

config.port.swapPortByNum

Syntax

```
swapPortByNum  portNum1 portNum2
```

Description

This command swaps two ports given the port numbers. The ports must be offline to perform this operation.

Parameters

This command has two required parameters:

portNum1	The port number, in hexidecimal format, of the desired port to be swapped.
portNum2	The port number, in hexidecimal format, of the desired port to be swapped.

Command example

```
Root> config port swapPortByAddr 1e 1f
```

config.port.type

Syntax

```
type portNumber portType
```

Description

This command sets the allowed type for a port.

A port can be configured as an F_Port, E_Port, or G_Port. On aSphereon 4300 orSphereon 4500, a port can also be an Fx_port or Gx_port.

NOTE
On the Sphereon 4300Switch, the E_Port, G_Port, and GX_Port options are not valid unless the Fabric Capable feature is enabled. For more information, see the*Sphereon 4300 Switch Installation and Service Manual* (620-000171).

The port configurations function as follows:

- *F_Port*—cannot be used as an interswitch link, but may attach to a device with an N_Port.
- *E_Port*—only other switches may attach to this type of port.
- *G_Port*—either a device or another switch may attach to this type of port.
- *Fx_Port* — allows Arbitrated Loop operation in addition to the functionality of an F_Port. (Sphereon 4300 and Sphereon 4500 only.)
- *Gx_Port*—allows Arbitrated Loop operation in addition to the functionality of an F_Port or an E_Port. (Sphereon 4300 and Sphereon 4500 only.)

Parameters

This command has two required parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portType	The type of the port. Valid values for the port type are: *eport* *fport* *gport* *fxport* (Sphereon 4300 and Sphereon 4500 only) *gxport* (Sphereon 4300 and Sphereon 4500 only)

Command example

```
Root> config port type 4 fport
```

config.security

Using the security command on the configuration branch, you can enter the security configuration branch. All commands under this branch operate on a particular security attribute.

Some security configuration commands (namely those under the fabricBinding branch) are different from other CLI commands in that they are not single action commands that take effect immediately. These commands implement a rudimentary membership list editor.

You work on a temporary copy of a membership list in the editor and can perform actions such as adding or deleting fabric members. The edited copy can then be activated to the fabric.

It should be noted that not all verification of membership lists can be made in the pending copy. Therefore, it is possible that you build up a pending membership list definition without errors, but encounter errors when saving to the fabric. It should also be noted that the state of the pending configuration must be set to *restrict* before you can make any changes to the (pending) fabric membership list.

config.security.authentication.interface

Using this command, the authentication interface is configured for Web and CLI users, OSMS, and devices. The authentication has two interfaces namely, Local and Radius, which can be used in three combinations namely, Local, Radius, and Radius then Local.

config.security.authentication.interface.api.outgoing

Syntax

```
outgoing  enabledState
```

Description

This command determines whether outgoing CHAP authentication is used on all API sessions. If this is enabled, the switch issues a CHAP challenge to authenticate all new API connections.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of outgoing CHAP authentication for API sessions. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security authentication interface api outgoing enable
```

config.security.authentication.interface.api.sequence

Syntax

```
sequence  method1 [method2]
```

Description

This command sets the sequence that the API interface uses for authentication. When the preferred method cannot be contacted, the backup method is used to authenticate the API session.

Parameters

This command has one required parameter, and one optional parameter:

method1	The preferred method of authentication. Accepted values are *local* or *RADIUS*.
method2	Optional. The backup method of authentication. This backup method is used when the preferred method cannot be contacted. Accepted value is *local*.

NOTE
A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command example

```
Root> config security authentication interface api sequence RADIUS local
```

config.security.authentication.interface.cli.sequence

Syntax

```
sequence  method1  [method2]
```

Description

This command sets the sequence that the CLI interface uses for authentication. When the preferred method cannot be contacted, the backup method is used to authenticate the CLI login.

Parameters

This command has one required parameter, and one optional parameter:

method1	The preferred method of authentication for the CLI interface. Accepted values are *local* or *RADIUS*.
method2	Optional. The backup method of authentication for the CLI interface. This backup method is used when the preferred method cannot be contacted. Accepted value is *local*.

NOTE
A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command example

```
Root> config security authentication interface cli sequence RADIUS local
```

config.security.authentication.interface.eport.outgoing

Syntax

```
outgoing  enabledState
```

Description

This command determines whether outgoing CHAP authentication is used on E_Port connections. If this is enabled, the switch issues a CHAP challenge to authenticate the remote end of the ISL.

NOTE
This command requires that the SANtegrity Authentication feature key be installed.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of outgoing CHAP authentication on all ISLs. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security authentication interface eport outgoing disable
```

config.security.authentication.interface.eport.sequence

Syntax

```
sequence  method1  [method2]
```

Description

This command sets the sequence that the E_Port interface uses for authentication. When the preferred method cannot be contacted, the backup method is used to authenticate the remote end of the ISL.

NOTE
This command requires that the SANtegrity Authentication feature key be installed.

Parameters

This command has one required parameter, and one optional parameter:

method1	The preferred method of authentication. Accepted values are *local* or *RADIUS*.
method2	Optional. The backup method of authentication. This backup method is used when the preferred method cannot be contacted. Accepted value is *local*.

NOTE
A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command example

```
Root> config security authentication interface eport sequence RADIUS local
```

config.security.authentication.interface.nport.outgoing

Syntax

```
outgoing  enabledState
```

Description

This command determines whether outgoing CHAP authentication is used on N_Port connections. If this is enabled, the switch issues a CHAP challenge to authenticate the remote device.

NOTE
This command requires that the SANtegrity Authentication feature key be installed.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of outgoing CHAP authentication on all ISLs. Accepted values for this parameter are *enable* or *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security authentication interface eport outgoing disable
```

config.security.authentication.interface.nport.sequence

Syntax

```
sequence  method1  [method2]
```

Description

This command sets the sequence that the N_Port interface uses for authentication. When the preferred method cannot be contacted, the backup method is used to authenticate the remote end of the ISL.

NOTE
This command requires that the SANtegrity Authentication feature key be installed.

Parameters

This command has one required parameter, and one optional parameter:

method1	The preferred method of authentication. Accepted values are *local* or *RADIUS*.
method2	Optional. The backup method of authentication. This backup method is used when the preferred method cannot be contacted. Accepted value is *local*.

NOTE
A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command example

```
Root> config security authentication interface nport sequence RADIUS local
```

config.security.authentication.interface.osms.outgoing

Syntax

```
outgoing  enabledState
```

Description

This command determines whether outgoing authentication is used on all OSMS requests. The OSMS key must be configured prior to setting the outgoing state to enabled.

NOTE
The SANtegrity Authentication feature key must be installed to configure the OSMS outgoing state.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of FCCT authentication. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security authentication interface osms outgoing 1
```

config.security.authentication.interface.osms.setKey

Syntax

```
setKey
```

Description

This command sets the FCCT key that is associated with the single OSMS username. This username is a static entry in the local authentication database. This user is not viewable. This command effectively sets the key that is used in all OSMS authenticated requests. This entry in the user database is only used for the OSMS interface, and cannot be changed.

After issuing this command, you are directed to a password prompt where you must enter the actual 16-byte key. After entering the new secret, you must confirm it in the following prompt. After confirmation, you are returned to the initial prompt from where the command was executed.

No characters are echoed back to the screen when entering/confirming a password.

NOTE
The SANtegrity Authentication feature key must be installed to configure the FCCT key.

Parameters

This command has no required parameters.

Command example

```
Root> config security authentication interface osms setKey
```

config.security.authentication.interface.serial.enhancedAuth

Syntax

```
enhancedAuth  enhancedAuthState
```

Description

This command sets the enhanced serial authentication state. Enhanced Serial Authentication requires you to enter a password when gaining access to the serial port interface.

Parameters

This command has one parameter:

enhancedAuthState	The enabled/disabled state of enhanced authentication on the serial port interface. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security authentication serial enhancedAuth enable
```

config.security.authentication.interface.show

Syntax

```
show  interface
```

Description

This command displays the settings in the local authentication database for a single interface.

NOTE
The SANtegrity Authentication feature key must be installed to view the E_Port, N_Port, and OSMS information.

Parameters

This command has one parameter:

interface	The interface that is displayed. Valid values for this parameter are: *cli* *web* *osms* *api* *serial* *eport* *nport*

Command example

```
Root> config security authentication interface show Web
```

Output example

The output for the *config.security.authentication.interface.show* command displays as follows:

```
Interface: Web
Outgoing:  N/A
Incoming:  N/A
Sequence:  Local, RADIUS
```

config.security.authentication.interface.web.sequence

Syntax

```
sequence  method1  [method2]
```

Description

This command sets the sequence used by the web interface for authentication. When the preferred method cannot be contacted, the backup method is used to authenticate the web login.

Parameters

This command has one required parameter, and one optional parameter:

method1	The preferred method of authentication for the CLI interface. Valid values are *local* and *RADIUS*.
method2	Optional. The backup method of authentication for the CLI interface. This backup method is used when the preferred method cannot be contacted. Accepted value is *local*.

NOTE
A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command example

```
Root> config security authentication interface cli sequence RADIUS local
```

config.security.authentication.port.override

Syntax

```
override  portNumber  [overrideState]
```

Description

This command sets the outgoing override state for a single port. This setting allows users to override the default outgoing authentication state for either the E_Port or N_Port interface. The default settings cause the port to use the outgoing state configure for the corresponding interface (E_Port or N_Port).

NOTE
This command requires that the SANtegrity Authentication feature key be installed.

Parameters

This command has one required parameter, and one optional parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
overrideState	The outgoing authentication state for the specified port. Valid values are *enable, disable*, or *default*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security authentication port override 138 enable
```

config.security.authentication.port.show

Syntax

```
show
```

Description

This command displays a table displaying the outgoing override state for each port.

Parameters

This command has no parameters.

Command example

```
Root> config security authentication port show
```

Output

This command displays all valid user names in the local database for the specified interface.

Port	The port number.
Override State	The outgoing authentication override state.

Output example

The output for the *config.security.authentication.port.show* command displays as follows:

```
Port       Override State
----       --------------
0          Default
1          Default
2          Enable
3          Default
4          Disable
```

config.security.authentication.RADIUS

Using this command, the Radius server database is configured for authentication. The timeout, attempts, and dead time values are also configured for Radius server.

config.security.authentication.RADIUS.attempts

syntax

```
attempts index  attempts
```

Description

This command configures the number of attempts by an authentication request to a RADIUS server if a response is not received before the timeout. After the transmit attempt limit is reached, the switch, if applicable, moves to the next defined RADIUS server. The default number of attempts is three.

Parameters

This command has two required parameters:

index	The index of the RADIUS sever (1-3) to change the transmit attempts value.
attempts	The number of transmit attempts. Valid values are between 1 and 100.

Command example

```
Root> config security authentication RADIUS attempts 3 20
```

config.security.authentication.RADIUS.deadtime

Syntax

```
deadtime  minutes
```

Description

This command configures the number of minutes a RADIUS server is marked as “dead”. If a RADIUS server does not respond to an authentication request, it can be marked as *dead* for a specified time interval. This may speed up authentication by eliminating timeouts and retransmissions. If no alternate RADIUS servers are available (when only one server is configured or when all are marked dead), then the deadtime is ignored. Deadtime may be 0 to 1440 minutes. The default is 0.

Parameters

This command has one required parameter:

minutes	The number of minutes a RADIUS server is marked “dead” before it is contacted again. Valid values are between 0 and 1440.

Command example

```
Root> config security authentication RADIUS deadtime 120
```

config.security.authentication.RADIUS.deleteServer

Syntax

```
deleteServer index
```

Description

This command removes a RADIUS server from the RADIUS server list. If you delete a server, and there are servers configured in higher numbered slots, these servers automatically move up to the first available slots.

Parameters

This command has one required parameter:

index	The index of the server to be removed.

Command example

```
Root> config security authentication RADIUS deleteServer 3
```

config.security.authentication.RADIUS.server

Syntax

```
server <index> <IP:port | [IPV6]:port>
```

Description

This command adds or modifies one RADIUS server at a given index that is used for authentication. Servers are queried in the order listed; the primary server must be the first one in the list.

There are three slots available for RADIUS servers. Servers are added into the list by the index value. The range is 1 to 3. If a server is added and there is an empty slot before that server, it is shifted up to the empty slot. The IP:port is the IP address and the UDP port on the RADIUS server.

NOTE
If you want to configure a RADIUS server without a key, you must specify the key as "". The set of double quotation marks are an empty string in the CLI.

Parameters

This command has one required parameter, and two optional parameters:

index	The index of the RADIUS server (1-3) to add or modify.
IP	The IP address of the server.(either V6 (hexadecimal colon based) format or V4 (4 bytes in dotted-decimal notation) format
port	The UDP port number.

Command example

```
Root> Config Security Authentication RADIUS server 2 [2019::221:456:21]:182
```

config.security.authentication.RADIUS.show

Syntax

```
show
```

Description

This command displays the current RADIUS server configuration.

Parameters

This command has no parameters.

Command example

```
Root>  Config Security Authentication RADIUS show

Deadtime:    0

Index    IP Address               Port   Attempts  Timeout
-----    ----------------------   -----  --------  -------
1          2001::12:453:21        172      3           4
2          2019::221:456:21       182      3           4
3          1291::ac1a:1cc0        192      3           4
```

Output

This command displays all three configured RADIUS servers.

Deadtime	The amount of time a server is marked as “dead”.

Server	The IP address and UDP port of the configured RADIUS server.(either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format))
Attempts	The number of transmit attempts.
Timeout	The timeout value for a server in seconds.

Output example

The output for the *config.security.authentication.RADIUS.show* command displays as follows:

```
Deadtime:     0

Index      IP Address     Port   Attempts       Timeout
-----      ------------- ----   ----------     -------
1          1.1.1.1        1111   3              2
2          2.2.2.2        2222   3              2
3
```

config.security.authentication.RADIUS.timeout

Syntax

```
timeout index seconds
```

Description

This command configures the waiting time, in seconds, for a response from the RADIUS server before retransmitting a packet. The default value is 4 seconds.

In extreme cases, where E_Port or N_Port authentication occur on a large number of ports with RADIUS, and a switch is coming online, users may need to increase the timeout value so that all the ports can log in.

For example, if all of the ports on an Intrepid 6140 Director are coming online at the same time and requiring authentication, some of the ports may not get an access_accept before they time out.

Parameters

This command has two required parameters:

index	The index of the RADIUS sever (1-3) to change the timeout value.
seconds	The number of seconds before the RADIUS server retransmits. Valid values are between 1 and 1000.

Command example

```
Root> config security authentication RADIUS timeout 3 360
```

config.security.authentication.switch.setSecret

Syntax

```
SetSecret
```

Description

This command sets the CHAP secret that is associated with the switch. This command effectively sets the secret for the local WWN username in the local authentication user database. The switch secret is used for all incoming CHAP challenges on the E_Port and N_Port interfaces.

After issuing this command, users are directed to a *password* prompt where the actual 16-byte secret is entered. After entering the new secret, it must be confirmed in the following prompt. After confirmation, users are returned to the initial prompt that the command was executed from.

No characters are echoed back to the screen when entering/confirming a password. See "Passwords and secrets" on page 13 for valid characters.

NOTE
The SANtegrity Authentication feature key must be installed to configure switch secret.

Parameters

This command has no required parameters.

Command example

```
Root> config security authentication switch setSecret
```

config.security.authentication.user

One of the fundamental concepts of the authentication portion of the CLI is that all secured interfaces have interchangeable users that are stored in a single local authentication user database. In the past, CLI supported authorization for only two username/password pairs (Administrator and Operator). These two username/password pairs were also unique to the CLI interface.

The present CLI lets you configure multiple users for their own interface, as well as for other management entities and FC connections. For this reason, the *security.userrights* branch of commands has been removed from the command tree.

config.security.authentication.user.add

Syntax

```
add  username  interface1  [interface2]
```

Description

This command adds a new user to the local authentication database. Each user can be assigned a combination of interfaces that authenticate the new username/password combination.

After executing this command, you are moved to a new password prompt where you enter a password and later, confirm it in the next prompt. After confirming the new password, you return to the initial prompt.

No characters are echoed back to the screen when entering/confirming a password.

All new users are assigned a role of *none*; a subsequent *role* command must be executed to assign a role. Web and CLI users must be assigned a role before they can access the CLI or web interfaces.

NOTE
The SANtegrity Authentication feature key must be installed to configure E_port and N_port usernames.

Parameters

This command has two required parameters and an additional interface parameter before the password parameter at the prompt after the command.

username	The new user name that is added to the local authentication database. If the entered user name already exists in the user database, an error is displayed. This parameter can be from 1-23 characters in length for an API, Web, or CLI username. E_Port and N_Port usernames must be entered as a standard colon-delimited WWN. All characters in the printable USASCII character set are valid with the exception of spaces, single quotation marks, and double quotation marks.
interfaces	A list of interfaces that is assigned to the associated username. Accepted values for this parameter are: *cli* *web* *api* *eport* *nport*
password	The password for the new login username. This parameter can be from 1-24 characters in length for a Web or CLI password. CHAP secrets and FCCT keys must be exactly 16 bytes long for API, OSMS, E_Port, and N_Port interfaces. This parameter is not echoed to the screen. See "Passwords and secrets" on page 13 for valid characters.

NOTE
Currently the only possible combination of multiple interfaces is Web and CLI.

Command example

```
Root> config security authentication user add 01:2A:3f:4:5:0:0 eport
```

config.security.authentication.user.delete

Syntax

```
delete  username
```

Description

This command deletes an entry from the local authentication database. Both the Web and CLI interfaces must have at least one valid username with an *Administrator* role.

Parameters

This command has one parameter:

username	A valid user name in the local authentication database.

Command example

```
Root> config security authentication user delete 01:2A:3f:4:5:0:0
```

config.security.authentication.user.modify

Syntax

```
modify  username  interface1 [interface2]
```

Description

This command modifies an existing user in the local authentication database. The user password and the combination of interfaces can be modified with this command. After executing this command, users are prompted to enter a password, similar to the behavior of the *user.add* command.

The role of a user remains the same unless the currently assigned role is invalid for the new combination of interfaces. If the role is no longer valid for an interface combination, the role is changed back to *none*. At least one username with an *Administrator* role must exist in the user database at all times for both the web and CLI interfaces.

NOTE
The SANtegrity Authentication feature key must be installed to configure E_port and N_port usernames.

Parameters

This command has two required parameters and an additional interface parameter before the password parameter at the prompt after the command:

username	The existing user name whose fields are modified in the local authentication database. If the entered user name does not exist in the user database, an error is displayed. This parameter can be from 1-23 characters in length for an API, web or CLI user name. E_Port and N_Port user names must be entered as a standard colon-delimited WWN. All characters in the printable USASCII character set are valid with the exception of spaces, single quotation marks, and double quotation marks.
interfaces	A list of interfaces that are assigned to the associated user name. Accepted values for this parameter are: *cli* *web* *api* *eport* *nport*.
password	The password for the existing username. This parameter can be from 1-24 characters in length for a Web or CLI user name. CHAP secrets must be exactly 16 bytes long for API, OSMS, E_Port, and N_Port interfaces. This parameter is not echoed to the screen. See "Passwords and secrets" on page 13 for valid characters.

NOTE
Currently the only possible combination of multiple interfaces is (Web and CLI) or (E_port or N_port).

Command example

```
Root> config security authentication user modify 01:2A:3f:4:5:0:0 nport
```

config.security.authentication.user.passExpTime

Syntax

```
passExpTime days
```

Description

This command configures the password expiry time for the management users of the switch or director. The value "0" specifies that the user password never expires.

Parameters

This command has one parameter:

days	A number from 0 - 3650 specifying the number of days after which the user password expires.

Command example

```
Root> config security authentication user passExpTime 90
```

config.security.authentication.user.role

Syntax

```
role  username privilegeLevel
```

Description

This command sets the role value associated with an existing user name. The role value can be set either to an administrator or an operator. This value defaults to *none* when the user is first added to the database. This value must be changed for all new CLI and web users before they are allowed access to their respective interfaces.

Parameters

This command has two required parameters:

username	A valid web or CLI username in the local authentication database.
privilegeLevel	The privilege level for a username. Currently only Web and CLI users can be assigned a role value. This parameter must be either *administrator* or *operator*.

Command example

```
Root> config security authentication user role 01:2A:3f:4:5:0:0 administrator
```

config.security.authentication.user.show

Syntax

```
show interface
```

Description

This command displays a single interface from the local authentication database. The API, E_Port and N_Port parameters do not have a password expiration time and the column is not displayed.

Parameters

This command has one optional parameter:

interface	The interface that is displayed. Accepted values for this parameter are: *cli* *web* *api* *eport* *nport*

Command example

```
Root> config security authentication user show web
```

Output

The output is displayed as a table with the following properties:

Username	The user name specified by the user.
Interfaces	The management interfaces that a user belong to.
Role	The management role of the user.
P-Exp	The number of days until the user's password expires.

NOTE
The P-Exp column is displayed only for Web and CLI interfaces.

Output example

The output for the *config.security.authentication.user.show* command displays as follows:

```
Interface: Web
Password Expiration Time: 365

Username            Interfaces         Role             P-Exp
------------------  -----------------  ---------------  ------
johndoe_1223        Web,CLI            Administrator    250
ewsOperator         Web                Operator         20
Operator            Web,CLI            Operator         365
```

config.security.fabricBinding

Fabric Binding functionality provided by the SANtegrity Binding feature helps bind the switch or director to specified fabrics so that they can communicate only with those fabrics included in the Fabric Binding Membership List (FBML). This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Fabric Binding Commands

The *config.security.fabricBinding* commands function in a different way from most CLI commands, which are single action commands that take effect immediately. Most of the Fabric Binding commands affect a temporary copy of an FBML in the work area called the Pending FBML. When this temporary copy is activated to the fabric, it is called the Active FBML.

NOTE
The EFCM Basic interface can change Fabric Binding status and FBMLs if it is used with the CLI.

Because not all the verification of the Pending FBML can occur on the temporary copy in the work area, it is possible, however unlikely, that the copy of the list encounters no errors until the list is activated to the fabric.

NOTE
A Sphereon 4300 Switch cannot participate in a fabric unless the Fabric Capable feature is enabled. For more information, refer to the *Sphereon 4300 Switch Installation and Service Manual* (620-000171).

Fabric Binding membership terminology

Two types of FBMLs are configured using the CLI:

- **Active FBML:** When fabric binding is active, the active FBML is the list of fabric members with which the product is allowed to communicate. If fabric binding is disabled, this list is empty.
- **Pending FBML:** A list used to configure an FBML before it is made active on the director or switch. Changes to the pending FBML are not implemented in the fabric until they are saved and activated using the *config.security.fabricBinding.activatePending* command as documented on page 82.

The following terms apply to the switches and directors that are part of FBMLs:

- *Local:* The switch or director that is being configured. This is a required FBML member.
- *Attached:* A switch or director that is currently in a fabric with the local switch or director. Any switch or director that is attached to the local switch or director is a required FBML member.
- *Unattached:* A switch or director that is not currently in a fabric with the local switch or director. These switches and directors are unattached if they have been added manually to the pending FBML, or if they are segmented from the local fabric.

Enable/Disable and Online state functions

For Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the switch or director is offline or online. Be aware of the following:

- Because switches are bound to a fabric by World Wide Name (WWN) and domain ID, the Insistent Domain ID is automatically enabled if Fabric Binding is enabled. If Fabric Binding is enabled and the switch or director is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director is offline, you can disable Insistent Domain ID, but this also disables Fabric Binding.
- You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding.

NOTE
Fabric Binding can be disabled when the switch is offline.

config.security.fabricBinding.activatePending

Syntax

```
activatePending
```

Description

This command activates the fabric binding configuration contained in the pending work area to the fabric. The pending FBML becomes the active FBML, and fabric binding is made functional.

NOTE
This command takes effect immediately. The CLI verifies the list before activating it to the fabric.

Parameters

This command has no parameters.

Command example

```
Root> config security fabricBinding activatePending
```

config.security.fabricbinding.addAttachedMembers

Syntax

```
addAttachedMembers
```

Description

This command adds all the current members of the fabric to the pending FBML. If the domain ID or WWN of a fabric member already exists in the list, it is not added.

Parameters

This command has no parameters.

Command example

```
Root> config security fabricbinding addAttachedMembers
```

config.security.fabricBinding.addMember

Syntax

```
addMember wwn domainId
```

Description

This command adds a new member to the pending FBML in the fabric binding work area, called the pending FBML. The number of entries is limited to the maximum available domain IDs for the fabric, which is 239.

NOTE
Changes from this command are not activated to the fabric until the *activatePending* command is issued.

Parameters

This command has two parameters:

wwn	The world wide name (WWN) of the member to be added to the Pending FBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).
domainId	The domain ID of the member to be added to the Pending FBML. Valid domain IDs range from 1 to 239.

Command example

```
Root> config security fabricBinding addMember AA:99:23:23:08:14:88:C1 2
```

config.security.fabricBinding.clearMemList

Syntax

```
clearMemList
```

Description

This command clears the Pending FBML in the working area. Members that are attached remain in the list because the pending FBML must contain all attached members to become active.

NOTE
This information is not saved to the fabric until the *activatePending* command is issued. When the list is cleared, the CLI automatically adds the managed switch to the Pending FBML.

Parameters

This command has no parameters.

Command example

```
Root> config security fabricBinding clearMemList
```

config.security.fabricbinding.deactivateFabBind

Syntax

```
deactivateFabBind
```

Description

This command deactivates the active FBML on the fabric. The Active FBML is erased when this command is executed.

NOTE
This command takes effect immediately in the fabric.

Parameters

This command has no parameters.

Command example

```
Root> config security fabricbinding deactivateFabBind
```

config.security.fabricBinding.deleteMember

Syntax

```
deleteMember wwn domainId
```

Description

This command removes a member from the Pending FBML in the fabric binding work area. The local member and attached members cannot be deleted from the list.

NOTE
Changes are not activated to the fabric until the *activatePending* command is issued.

Parameters

This command has two parameters:

wwn	The WWN of the member to be removed from the Pending FBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).
domainId	The domain ID of the member to be removed from the Pending FBML. Valid domain IDs range from 1 to 239.

Command examples

```
Root> config security fabricBinding deleteMember AA:99:23:23:08:14:88:C1 2
```

config.security.fabricBinding.replacePending

Syntax

```
replacePending
```

Description

This command replaces the Pending FBML with the fabric binding configuration that is currently loaded on the fabric.

Parameters

This command has no parameters.

Command example

```
Root> config security fabricBinding replacePending
```

config.security.fabricBinding.showActive

Syntax

```
showActive
```

Description

This command displays the fabric binding configuration (active FBML) saved on the fabric. It performs the same function as “show.preferredPath.showState” on page 268.

Parameters

This command has no parameters.

Command example

```
Root> config security fabricBinding showActive
```

Output

This command displays the following fabric binding configuration data:

Domain ID	The domain ID of the FBML member. Valid domain IDs range from 1 to 239.
WWN	The WWN of the FBML member in colon-delimited hexadecimal notation.
Attachment Status	The attachment status of the FBML member. Possible values are Local, Attached, and Unattached. For more information, see "Fabric Binding membership terminology" on page 81.

Output example

The output from the *config.security.fabricBinding.showActive* command displays as follows.

```
Domain 1  (20:30:40:50:60:70:8F:1A) (Local)
Domain 3  (00:11:22:33:44:55:66:77) (Unattached)
Domain 2  (88:99:AA:BB:CC:DD:EE:FF) (Attached)
Domain 14 (11:55:35:45:24:78:98:FA) (Attached)
```

config.security.fabricBinding.showPending

Syntax

```
showPending
```

Description

This command displays the pending FBML, which may not reflect what is active on the fabric.

Parameters

This command has no parameters.

Command example

```
Root> config security fabricBinding showPending
```

Output

The fabric binding configuration data is displayed as a table that includes the following properties of the Pending FBML.

Domain ID	The domain ID of the FBML member. Valid domain IDs range from 1 to 239.
WWN	The WWN of the FBML member in colon-delimited hexadecimal notation.
Attachment Status	The attachment status of the FBML member. Possible values are Local, Attached, and Unattached. For more information, see "Fabric Binding membership terminology" on page 81.

Output example

The output from the *config.security.fabricBinding.showPending* command displays as follows.

```
Domain 1  (20:30:40:50:60:70:8F:1A) (Local)
Domain 3  (00:11:22:33:44:55:66:77) (Unattached)
Domain 2  (88:99:AA:BB:CC:DD:EE:FF) (Attached)
Domain 14 (11:55:35:45:24:78:98:FA) (Attached)
```

config.security.portBinding

The Port Binding CLI commands enables users to bind a specific switch or director port to the WWN of an attached node, switch, or director for exclusive communication.

config.security.portBinding.bound

Syntax

```
bound portNumber portBindingState
```

Description

This command sets the port binding state for a given port.

Parameters

This command has two parameters:

portNumber	The port number for which the port binding state is being set. Valid port number values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portBindingState	The active/inactive state of the port binding. Valid values are *true* and *false*. *true* sets the port binding to active. The specified port is bound to the WWN configured with the *config.security.portBinding.wwn* command. If no WWN has been configured, no devices can log in to that port. *false* sets the port binding to inactive. Any device is free to connect to the specified port in this state, regardless of the WWN setting. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> config security portBinding bound 4 true

Root> config security portBinding bound 4 1
```

config.security.portBinding.show

Syntax

```
show portNumber
```

Description

This command shows port binding configuration for a single port.

Parameters

This command has one parameter:

portNumber	The port number for which the port binding configuration is displayed. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> config security portBinding show 4
```

Output

The port binding configuration date is displayed as a table that includes the following properties:

Port Number	The port number.
WWN Binding	The state of port binding for the specified port: *active* or *inactive*.
Bound WWN	The WWN of the device bound to the specified port. If this field is blank, no device has been bound to the specified port.

Output example

The output from the *config.security.portBinding.show* command displays as follows.

```
Port Number:      4
WWN Binding:      Active
Bound WWN:        AA:99:23:23:08:14:88:C1
```

config.security.portBinding.wwn

Syntax

```
wwn portNumber boundWwn
```

Description

This command configures the single device WWN to which a port is bound.

Parameters

This command has two parameters:

portNumber	The port number for which the bound WWN is being set. Valid port number values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
boundWwn	The WWN of the device that is being bound to the specified port. The value must be entered in colon-delimited hexadecimal notation (for example, 11:22:33:44:55:66:AA:BB). If the boundWwn is configured and the portBindState is: *Active*—only the device described by boundWwn can connect to the specified port. *Inactive*—the WWN is retained, but any device can connect to the specified port. Instead of the WWN, either of two values can be entered in this parameter: *attached* automatically configures the currently attached device WWN as the bound WWN. *remove* changes the WWN to the default value, 00:00:00:00:00:00:00:00. Even though this removes the WWN-port association, if the portBindingState value set with the *config.security.portBinding.bound* command is still *true* (the port binding is active), other devices are prevented from logging in to this port. To allow other devices to log in to this port, use the *config.security.portBinding.bound* command to set the portBindingState parameter to *false*.

Command examples

```
Root> config security portBinding wwn 4 AA:99:23:23:08:14:88:C1

Root> config security portBinding wwn 4 attached

Root> config security portBinding wwn 4 remove
```

config.security.ssh

The Secure Shell feature provides an encrypted connection between an SSH client and the switch. The switch acts as an SSH server to provide secure access to the CLI. This feature solves the Telnet issue of user IDs and passwords being passed “in clear text” between the Telnet and switch. Telnet results in a lack of security as anyone having access to the IP network or an intermediate IP network, can intercept the user ID and password and then gain unauthorized access to the switch.

config.security.ssh.resetKeys

Syntax

```
resetKeys
```

Description

This command resets the SSH Public/Private keys. After resetting the keys, the new keys are generated immediately and do not wait until the next user session.

Parameters

This command has no parameters

Command example

```
Root> config security ssh resetKeys
```

config.security.ssh.setRenegotiationMB

Syntax

```
setRenegotiationMB megabytes
```

Description

This command sets the number of megabytes that can be transferred using SSH before the SSH session keys are renegotiated.

It does not affect the SSH public or private key. Instead, it indicates that new SSH session keys should be renegotiated for the current SSH connection after this number of megabytes has been transferred between the SSH client and the switch. The renegotiation is transparent to the user. The purpose of renegotiation is to increase security by limiting the amount of data encrypted with the same negotiated SSH parameters.

Parameters

This command has one parameter:

megabytes	The number of megabytes transferred before the SSH session is renegotiated. Valid values are *1 (MB)* to *1000 (MB)* or *0 (no renegotiation)*. The default value is 0.

Command example

```
Root> config security ssh setRenegotiationMB 128
```

config.security.ssh.setState

Syntax

```
setState sshEnableState
```

Description

This command sets the enabled state for the SSH interface. For an SSH client connection to be accepted, the state must be set to *enable*; otherwise, only Telnet can be accepted. Both SSH and Telnet cannot be enabled at the same time.

Parameters

This command has one parameter:

sshEnableState	The enabled/disabled state of the SSH interface. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security ssh setState enable
```

config.security.ssh.show

Syntax

```
show
```

Description

This command displays the SSH Public key in PEM format, its MD5 fingerprint, its SHA-1 fingerprint, SSH, and Telnet state for the CLI interface.

Parameters

This command has no parameters.

Command example

```
Root> config security ssh show
```

Output

The output of the *config.security.ssh.show* command displays the following data:

SSH	The enabled/disabled status of the SSH interface to CLI. Possible values are *enabled* or *disabled*.
Telnet	The enabled/disabled state of the Telnet interface to CLI. Possible values are *enabled* or *disabled*.
Renegotiation MB	The SSH MB limit before renegotiation to take place.
Public Key	The SSH public key's PEM fingerprint.
MD5 Fingerprint	The SSH public key's MD5 fingerprint.
SHA-1 Fingerprint	The SSH public key's SHA-1 fingerprint.

Output example

```
SSH:                 enabled
Telnet:              disabled
Renegotiation MB:    0

Public Key:
-----BEGIN PUBLIC KEY-----
MIHxMIGoBgcqhkjOOAQBMIGcAkEAt+W14KwlGwHMzV15vSBxNXpMckhr3gpVOAkq/6ACLZDDGD8Izlq+m
xK0afu7Ir5hexE9v5potwk0fk38kwPhMQIVAN/hih31RuuaQTNgQNVAtrTDkFBVAkBaYRsm4Fj7/4i8Lt
7OydKJcYTMAJhJ71UboAVFpmfyVpCQOh3RFK9HfNYJYjkTaSTB3QQt9Hz1HilU/oKSx8aBA0QAAkEAh0B
1piZzDUfXmLuKsIf2sst7lSXfgtkxg85dfpPyJMSqM6M93D5wM3Nh/O54tSefEDi559HftVsX4YFKmYXV
+w==
-----END PUBLIC KEY-----

MD5 Fingerprint:
d1:f2:aa:9d:ec:92:de:38:75:d0:47:2f:9c:cb:b2:02

SHA-1 Fingerprint:
dc:f5:33:c8:e0:8b:01:4b:ce:b5:68:a1:55:2b:dd:8f:a5:5c:8c:26
```

config.security.switchAcl

The access control list (ACL) feature allows the administrator to configure a set of IP addresses that are allowed to make an IP management connection to the switch or director.

config.security.switchAcl.addRange

Syntax

```
addRange startIPAddress endIPAddress
```

Description

This command adds a new range of IP addresses to the access control list.

Parameters

This command has the following parameters:

startIPAddress	The starting IP Address of the range to be added. The address must be entered in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format) (such as, 10.0.0.0).
endIPAddress	The ending IP Address of the range to be added. The address must be entered in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format) (such as, 10.0.0.0).

NOTE
The maximum number of entries in this command is 32.

Command example

```
Root> config security switchacl addrange 2001::222:192:11 2913:222::271
```

config.security.switchAcl.deleteRange

Syntax

```
deleteRange startIPAddress endIPAddress
```

Description

This command deletes a range of IP addresses from the access control list. This range must exactly match one of the existing ranges in the access control list.

Parameters

This command has the following parameters:

startIPAddress	The starting IP Address of the range to be deleted. The address must be entered in dotted decimal form (such as, 10.0.0.0). *all* - Using the optional “all” parameter by itself removes all of the entries from the access control list.
endIPAddress	The ending IP Address of the range to be deleted. The address must be entered in dotted decimal form (such as, 10.0.0.0).

Command example

```
Root> config security switchAcl deleteRange 10.0.0.0 10.0.0.2
```

config.security.switchAcl.setState

Syntax

```
setState aclEnabledState
```

Description

This command enables or disables the access control list.

Parameters

This command has one parameter:

aclEnabledState	The enabled/disabled state of the access control list. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security switchAcl setState 1
```

config.security.switchAcl.show

Syntax

```
show
```

Description

This command displays the contents of the access control list.

Parameters

This command has no parameters.

Command example

```
Root> config security switchacl show
Switch IP ACL State:    Disabled

Starting IP Address            Ending IP Address
-------------------------  ---------------------
2001::222:192:11               2913:222::271
2001:: 1601:117                   2032::123

Log                                 State
--------------------------          --------
Event Log                             Disabled
Open Trunking Re-Route Log            Disabled
Link Incident Log                     Disabled
```

```
Threshold Alert                         Disabled
Security Log                            Disabled
Audit Log                               Disabled
Fabric Log                              Disabled
Embedded Port Frame Log                 Disabled
```

Output

This command displays the following access control list information:

Starting IP Address	The starting IP Address of the range in the access control list.(either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format)).
Ending IP Address	The ending IP Address of the range in the access control list.(either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format)).

Output example

The output from the *config.security.switchAcl.show* command displays as follows.

```
ACL State:  Disabled

Starting IP Address        Ending IP Address
-------------------        -----------------
110.80.1.1                 110.80.255.255
110.81.1.10                110.81.1.255
200.11.15.1                200.11.255.128
```

config.security.switchBinding

Switch Binding CLI commands allow users to enable the switch or director to communicate only with nodes, switches, and directors that are listed on the Switch Binding Membership List (SBML). Switch Binding is available only if the SANtegrity Binding feature is installed.

When an unauthorized WWN attempts to log in, it is denied a connection and an event is posted to the Event Log. This provides security in environments that include a large number of nodes, switches, and directors by ensuring that only the specified set of WWNs are able to attach to the managed product.

Enable, Disable and Online State Functions

For Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features.

- Switch Binding can be enabled or disabled whether the switch or director is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- If Enterprise Fabric Mode is enabled and the switch or director is online, Switch Binding cannot be disabled.
- If Enterprise Fabric Mode is enabled and the switch or director is offline, users can disable Switch Binding, but this also disables Enterprise Fabric Mode.
- WWNs can be added to the SBML regardless of whether Switch Binding is enabled or disabled.

config.security.switchBinding.addMember

Syntax

```
addMember wwn
```

Description

This command adds a new member to the SBML. A maximum number of 256 members may be added to the SBML.

Parameters

This command has one parameter:

wwn	The switch or N_Port device WWN of the member to be added to the SBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).

Command example

```
Root> config security switchBinding addMember AA:99:23:23:08:14:88:C1
```

config.security.switchBinding.deleteMember

Syntax

```
deleteMember wwn
```

Description

This command removes a member from the SBML. You cannot remove any member currently logged into the switch or director.

Parameters

This command has one parameter:

wwn	The switch or N_Port device WWN of the member to be removed from the SBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00). You may also enter *all* for this argument to clear the SBML completely. Note that you cannot clear a WWN that is currently logged into the switch.

Command example

```
Root> config security switchBinding deleteMember AA:99:23:23:08:14:88:C1
```

config.security.switchBinding.setState

Syntax

```
setState switchBindingState
```

Description

This command sets the switch binding state on the switch.

Parameters

This command has one parameter:

switchBindingState	The switch binding state for the switch. Valid values are: *disable* - Disables switch binding. Devices (servers, storage, and other switches) are allowed to connect to the switch without restrictions. *eRestrict* - Enables switch binding and restricts E_Port connections. E_Ports are prevented from forming ISL connections unless explicitly identified in the SBML. F_Port connections are allowed without restriction. *fRestrict* - Enables switch binding and restricts F_Port connections. Server and (or) storage devices are prevented from forming F_Port connections with the switch unless explicitly identified in the SBML. E_Ports are allowed to form ISL connections without restriction. *allRestrict* - Enables switch binding and restricts E_Port and F_Port connections. Both E_Ports and F_Ports prohibit connections with all devices unless explicitly identified in the SBML.

Command example

```
Root> config security switchBinding setState allRestrict
```

config.security.switchBinding.show

Syntax

```
show
```

Description

This command displays the switch binding configuration.

Parameters

This command has no parameters.

Command example

```
Root> config security switchBinding show
```

Output

This command displays the following switch binding configuration data:

switchBindingState	The state of switch binding, which can have the following values: *Disabled* *Enabled and Restricting F_Ports* *Enabled and Restricting E_Ports* *Enabled and Restricting All Ports*
Switch Binding Membership List	The WWNs of members of the SBML saved on the switch.

Output example

The output from the *config.security.switchBinding.show* command displays as follows:

```
Switch Binding State:   Enabled and Restricting E_Ports
00:11:22:33:44:55:66:77
88:99:AA:BB:CC:DD:EE:FF
11:55:35:45:24:78:98:FA
```

config.security.ssl

The Secure Socket Layer (SSL) protocol ensures secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one or both ends of the transactions using a public key and private key concept. The public key is issued by the web server to the web browser, which uses this key to encrypt its URL and other HTTP data and sends it back to the web server. This encrypted key is decrypted by the web server using a private key.

config.security.ssl.generateKeys

Syntax

```
generateKeys validDays
```

Description

This command generates a new SSL public certificate and private key. The certificate is valid for the number of days specified. Unlike the *resetKeys* command, this command does not wait until the next SSL connection to generate the key. Instead, it generates the certificate and private key immediately.

The purpose for generating new keys is to improve the security of the SSL connections in case the private key has been compromised. This is considered to be unlikely, but the generation of new keys is usually performed periodically as a matter of security policy.

Once a new certificate and private key are generated, you see a message upon SSL connection that indicates that the new certificate is unrecognized. You can then choose to accept or reject the connection. The web browser warning message typically provides an MD5 or SHA-1 fingerprint that allows you to verify the connection before continuing.

If you choose, you can manually verify the fingerprint shown by the web browser by comparing it with the fingerprint provided at the end of the *config.security.ssl.show* command.

The web browser displays another warning upon expiration of the certificate. At this point, you can either choose to continue or cancel, despite the expiry date.

NOTE
The generation of the certificate and private key can be CPU intensive; therefore it is recommended that this be performed outside of peak hours.

Parameters

This command has one parameter:

validDays	The validity of the key in days. Valid values are 30 to 3650 days. This value should be selected as part of a security policy. The certificate and private key should be regenerated before this date expires.

Command example

```
Root> config security ssl generateKeys 50
```

config.security.ssl.resetKeys

Syntax

```
resetKeys
```

Description

This command resets the SSL public certificate and private encryption key to factory default values. For the next SSL connection, a new certificate and private key is created. The new certificate is valid for one year. The web browser displays a notification when the certificate expires. At this point, you can either choose to continue or cancel, despite the expiry date.

Parameters

This command has no parameters.

Command example

```
Root> config security ssl resetKeys
```

config.security.ssl.setRenegotiationMB

Syntax

```
setRenegotiationMB megabytes
```

Description

This command sets the megabytes that can be transferred using SSL before the SSL session is automatically renegotiated. This renegotiation increases security by limiting the amount of data encrypted with the same negotiated SSL parameters.

This command does not affect the SSL certificate or private key. Instead, it indicates that a new SSL session should be renegotiated for the current SSL connection after the specified megabytes have been transferred between the SSL client and the switch. The renegotiation is transparent to the user.

Parameters

This command has one parameter:

megabytes	The number of megabytes transferred before the SSL session is renegotiated. Valid values are *50 (MB)* to *1000 (1000 MB or 1 GB)* or *0*.

Command example

```
Root> config security ssl setRenegotiation 50
```

config.security.ssl.setWebState

Syntax

```
setWebState sslEnabledState
```

Description

This command enables the SSL for web interface. For a secure (https://) connection to be accepted, the state must be set to *enable*; otherwise, only http://" is accepted. The default WebState access is non-secure.

If SSL is disabled, the https:// URL is rejected. If SSL is enabled, both the http:// and https:// are accepted. However, the http:// URL immediately redirects the web browser to the https:// URL so that all web communication is secure.

Parameters

This command has one parameter:

sslEnabledState	The enabled/disabled state of the SSL. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security ssl setWebState 0
```

config.security.ssl.setAPIState

Syntax

```
setAPIState sslEnabledState
```

Description

This command sets the enabled state for the SSL API interface. The default API access is non-secure. If SSL is enabled, there is no visual indication provided to the end user.

Parameters

This command has one parameter:

sslEnabledState	The enabled/disabled state of the SSL API interface. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config security ssl setAPIState 1
```

config.security.ssl.show

Syntax

```
show
```

Description

This command displays the SSL certificate, its MD5 and SHA-1 fingerprints, and the SSL enabled states for the web and API interfaces.

Parameters

This command has no parameters.

Command example

```
Root> config security ssl show
```

Output

Web Enable State	The SSL enabled state for the web interface.
API Enable State	The SSL enabled state for the API interface.
Renegotiation MB	The SSL MB limit before renegotiation takes place.
Certificate	The SSL certificate.
PEM	The SSL certificate in Privacy Enhanced Mail (PEM) format.
MD5 Fingerprint	The MD5 fingerprint of the SSL certificate.
SHA-1 Fingerprint	The SHA-1 Fingerprint of the SSL certificate.

Output example

```
Web SSL State:       Disabled
API SSL State:       Enabled
Renegotiation MB:    50

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1115038194 (0x427621f2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=Switch Serial Number TEST4500, O=Switch Serial Number
TEST450
0
        Validity
            Not Before: May  2 12:49:54 2005 GMT
            Not After : Jun 21 12:49:54 2005 GMT
        Subject: CN=172.26.22.212, O=Switch Serial Number TEST4500
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:ba:7a:de:88:4a:6a:91:49:10:8e:0e:d5:a0:93:
                    43:3f:f4:79:7a:88:a2:c1:17:51:28:c9:bd:2d:d2:
                    e8:ea:d4:86:b0:12:59:7b:06:f4:19:4b:25:a1:06:
                    a1:31:e2:16:9d:e3:c1:d7:47:0e:ab:ef:53:b7:81:
                    82:16:49:21:5f
```

```
                Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Subject Alternative Name:
                DNS:172.26.22.212
        Signature Algorithm: sha1WithRSAEncryption
            5a:6b:7d:b9:35:3e:13:53:61:38:be:bb:54:39:18:39:23:ac:
            52:a1:bf:d4:87:79:22:2c:ee:fb:3e:40:89:3d:97:9e:c7:b3:
            7f:f2:4f:2e:af:67:3c:08:63:71:1b:b3:85:7b:dc:81:a8:3c:
            85:da:84:07:62:2b:a5:83:92:aa


PEM:
-----BEGIN CERTIFICATE-----
MIIBoDCCAUqgAwIBAgIEQnYh8jANBgkqhkiG9w0BAQUFADBQMSYwJAYDVQQDEx1T
d2l0Y2ggU2VyaWFsIE51bWJlciBURVNUNDUwMDEmMCQGA1UEChMdU3dpdGNoIFNl
cmlhbCBOdW1iZXIgVEVTVDQ1MDAwHhcNMDUwNTAyMTI0OTU0WhcNMDUwNjIxMTI0
OTU0WjBAMRYwFAYDVQQDEw0xNzIuMjYuMjIuMjEyMSYwJAYDVQQKEx1Td2l0Y2gg
U2VyaWFsIE51bWJlciBURVNUNDUwMDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC6
et6ISmqRSRCODtWgk0M/9Hl6iKLBF1Eoyb0t0ujq1IawEll7BvQZSyWhBqEx4had
48HXRw6r71O3gYIWSSFfAgMBAAGjHDAaMBgGA1UdEQQRMA+CDTE3Mi4yNi4yMi4y
MTIwDQYJKoZIhvcNAQEFBQADQQBaa325NT4TU2E4vrtUORg5I6xSob/Uh3kiLO77
PkCJPZeex7N/8k8ur2c8CGNxG7OFe9yBqDyF2oQHYiulg5Kq
-----END CERTIFICATE-----

MD5:
1F:AC:B8:FF:BD:92:F0:13:E7:43:5E:AB:7F:C4:2D:E6

SHA-1:
5E:4A:0E:91:33:4B:10:75:00:EE:33:A8:AD:55:14:46:F4:E3:6B:43
```

config.snmp

The M-EOS provides an additional level of security to the existing SNMP framework by supporting SNMPv3 in addition to SNMP versions 1 and 2, which authenticate the SNMP requests based on the community string.

SNMPv3 provides security and access control by supporting a set of authentication protocols (HMAC-MD5-96, HMAC-SHA-96) and a privacy protocol (CBC-DES symmetric encryption protocol). The security and access based on the User-based Security Model (USM) and View-based Access Control Model (VACM) requires using multiple tables: User Table, Access Table, Security-to-Group Table and Target Table. The M-EOS CLI provides commands to configure these tables and enables or disables v1-v2/v3 support.

The SNMP client must be configured according to the security and access settings on the agent. To ensure that existing v1 and v2 community strings can continue to communicate with the agent, they must be configured appropriately in SNMPv3.

NOTE
Before enabling SNMPv3, ensure that all desired communities are configured for SNMPv3 access. If existing community strings are not configured for SNMPv3, then existing SNMP access is lost.

The authentication/privacy key (password) configured for an SNMPv3 User on a switch is not localized. Therefore, the authentication/privacy key configured in the SNMP management application must be configured as a non-localized authentication/privacy key in ASCII format. For more information on localization, refer to *http://www.ietf.org/rfc/rfc3414.txt?number=3414.*

config.snmp.addAccessEntry

Syntax

```
addAccessEntry index secModel secLevel groupName
```

Description

This command adds an entry to the access table.

Parameters

This command has four parameters:

index	The index of the access entry. Valid values are 1 to 12.
secModel	The Security Model to be used for this entry. Possible values for this parameter are *v1*, *v2* and *usm*.
secLevel	The security level for this entry. It specifies whether the entry requires authentication and/or privacy. The possible values for this parameter are *authPriv*, *authNoPriv* and *noAuthNoPriv*.
groupName	The Group Name for the particular Access table entry. The maximum length for the group name is 32 characters and all characters in ISO Latin 1 character set are valid for the group name. Duplicate group names are allowed as long as the groupName, secModel, and secLevel for those entries can specify a Unique Access Table Entry (At least one field differs when the group name is the same).

Using Authentication (Auth): The authentication protocols such as HMAC-MD5 or HMAC-SHA are used to calculate the hash value for the packet and this calculated Hash value is sent along with the packets as part of the SNMPv3 Header.

Using privacy (priv): The data part of the packet is encrypted using a privacy protocol such as DES. Privacy without authentication is not allowed by SNMPv3. Presently, the only authentication protocols supported are HMAC-MD5 and HMAC-SHA. DES is the only privacy protocol that is supported.

Command example

```
Root> config snmp addaccessentry 1 v2 authpriv joe
```

config.snmp.addAccessViews

Syntax

```
addAccessViews index secModel secLevel groupName
```

Description

This command sets the views for a particular entry in the access table. This command has a one-to-one mapping with the config.snmp.addAccessEntry command.

Parameters

This command has four parameters:

index	The index of the access entry. Valid values are 1 to 12.
readView	The name of the Read View. See the View table for possible values.
writeView	The name of the Write View. See the View table for possible values.
notifyView	The name of the Notify View. See the View table for possible values.

Command example

```
Root> config snmp addaccessview 1 internet management experimental
```

config.snmp.addCommunity

Syntax

```
addCommunity commIndex commName writeAuthorization trapRecipient udpPortNum
```

Description

This command adds an SNMP community to the SNMP configuration and specifies a trap recipient.

Parameters

This command has five parameters. Up to six community names and trap recipients may be defined as follows:

commIndex	The community to be created or edited. Valid values are integers in the range 1–6.
commName	The community name of the community specified by *commIndex*. The community name must not exceed 32 characters in length. Valid characters include all those in the ISO Latin-1 character set. Duplicate community names are allowed but the corresponding *writeAuthorization* values must match.

writeAuthorization	The write authorization state of the community. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.
trapRecipient	The IP address of the trap recipient. Values must be either in V6 (hexadecimal colon based) format or V4 (4 bytes in dotted-decimal notation) format.
udpPortNum	The User Datagram Protocol (UDP) port number to which the director sends traps for each recipient. The value can be a decimal number or *default*. The default value is 162. Valid values include all legal UDP port numbers.

Command example

```
Root> config snmp addcommunity 1 public 1 2001::221:12 172
```

config.snmp.addTargetParams

Syntax

```
addTargetParams index secName grpName model level
```

Description

This command associates additional USM configuration values to the trap recipient. These values are required to perform the access control validation before sending the trap messages. This command operates on an entry created by one of the following commands: *addv1Target*, *addv2Target*, or *addv3Target*.

Parameters

This command has five parameters:

index	The index of the Target entry. Valid values are indices already created using one of the addv1Target, addv2Target or addv3Target commands.

secName	The Security Name to be used for the corresponding trap entry. The maximum length for the security name is 32 characters and all characters in the ISO Latin-1 character set are valid. This name is the same as the User name in the USM user table. Refer to the command *config.snmp.addUserEntry*.
secModel	The security model to be used for this entry. Possible values for this parameter are *v1*, *v2* and *usm*.
secLevel	The security level for this entry. It specifies whether the entry requires authentication and/or privacy. The following values are valid: *authPriv:* Requires both authentication and privacy *authNoPriv:* Requires authentication, but no privacy *noAuthNoPriv*: Requires neither authentication nor privacy

Using Authentication (Auth): The authentication protocols such as HMAC-MD5 or HMAC-SHA are used to calculate the hash value for the packet and this calculated Hash value is sent along with the packets as part of the SNMPv3 Header.

Using privacy (priv): The data part of the packet is encrypted using a privacy protocol such as DES. Privacy without authentication is not allowed by SNMPv3. Presently, the only authentication protocols supported are HMAC-MD5 and HMAC-SHA. DES is the only privacy protocol that is supported.

Command example

```
Root> config snmp addtargetparams 1 joe v1 authpriv
```

config.snmp.addUserEntry

Syntax

```
addUserEntry index username authPtcl privPtcl
```

Description

This command adds a User-based Security Model (USM) user entry to the User Table (RFC 2574). It also specifies the authentication protocol and privacy protocol for this user.

Parameters

This command has four parameters:

index	The index of the target entry. Valid values are 1 to 6.
username	The User Name (also referred to as Security Name). The maximum length for the User Name is 32 characters. All characters in the ISO-Latin 1 character set are valid. Duplicate entries are not allowed.
authPtcl	The authentication protocol being used by this user. The possible values for this parameter are *noauth*, *md5* and *sha*. The value *noauth* specifies that this user does not use any authentication protocol. The values *MD5* and *SHA* specify that the respective protocols that are used for authentication. If this parameter is set to MD5 or SHA, then after the command has been executed, you will be prompted twice for a 16 byte MD5 key, or a 20 byte SHA key.
privPtcl	The privacy protocol being used by this user entry. This parameter can take the values *noprivacy* and *des*. If this parameter is set to *DES*, then after the prompt for the authentication key, you will be prompted twice for a 16 byte DES key.

NOTE
Privacy protocol can be selected only when authentication is enabled.

Command example

```
Root> config snmp adduserentry 1 smith noauth noprivacy

Root> config snmp adduserentry 1 smith md5 des
Auth Password:16 byte key (eg: 1234 5678 9123 4567)
Confirm: Retype the auth password
Privacy Password:16 byte key (eg: 1234 5678 9123 4567)
Confirm: Retype the privacy password
```

config.snmp.addV3Group

Syntax

```
addV3Group index username secModel groupName
```

Description

This command configures an entry in the Security-to-Group table. This table is used to map a user to a group and a security model.

Parameters

This command has four parameters:

index	The index of the user entry. Valid values are 1 to 6.
username	The User Name (also referred as Security Name) for this entry. The maximum length for this User Name is 32 characters. All characters in the ISO-Latin 1 character set are valid for this user name. The same user can be mapped to the same group if the security model is different or, mapped to the same security model with a different group name.
secModel	The Security Model to be used for this entry. Possible values for this parameter are *v1*, *v2* and *usm*.
groupName	The name of the group to which the v3 User belongs or is mapped. One or more users can be grouped under a single Group Name. Maximum length for Group Name is 32 characters and all characters in the ISO Latin-1 character set are valid. Duplicate values are also allowed.

Command example

```
Root> config snmp addV3Group 1 smith v2 smithGroup
```

Output example

The output shows the same user mapped to different groups and security models.

```
Config.SNMP> addv3Group 1 smith v1 smithGroup
Config.SNMP> addv3Group 2 smith USM smithGroup
Config.SNMP> addv3Group 3 smith USM smithOtherGroup
   Config.SNMP> showV3Group
   SNMPv3 State:    Disabled
   Index  Username                         Model  Group Name
   -----  -------------------------------  -----  ----------
   1      smith                            V1     smithGroup
   2      smith                            USM    smithGroup
   3      smith                            USM    smithOtherGroup
```

config.snmp.addV1Target

Syntax

```
addV1Target index community [IP] [udpNum]
```

Description

This command configures a v1 community string. The IP address and port number of a v1 trap recipient can be optionally specified. The community string can be used for v1 access only if mapped to a security and group name.

Parameters

This command has four parameters. The last two are optional.

index	The index of the target entry. Valid values are 1 to 6.
community	The community string of the target entry. The maximum length of the community string is 32 characters. All characters in the ISO Latin-1 character set are valid for community names. Duplicate community names are allowed, but the corresponding security names (refer to the command *config.snmp.addTargetParams*) must also match.
IP	The address of the trap recipient shown in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format).
udpNum	The UDP port number of the trap recipient, to which the SNMP agent sends the traps. This value is expressed in decimal and the default value is 162. The default number is assumed if this field is replaced with *default*. All legal UDP port numbers are allowed. If the IP address is specified and this parameter is not specified, it is set to the default value.

Command example

```
Root> config snmp addV1target 2 abc 4211::234:22:2124:22 182
```

config.snmp.addV2Target

Syntax

```
addV2Target index community [IP] [udpNum]
```

Description

This command configures a v2 community string. The IP address and port number of a v2 trap recipient can be optionally specified. The community string can be used for v2 access only if mapped to a security and group name.

Parameters

This command has four parameters. The last two are optional.

index	The index of the target entry. Valid values are 1 to 6.
community	The community string of the target entry described by the index. The maximum length of the community string is 32 characters. All characters in the ISO Latin-1 character set are valid for community names. Duplicate community strings are allowed.
IP	The IP address of the trap recipient shown in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format).
udpNum	The UDP Port Number of the trap recipient to which the SNMP agent sends the traps. This value is expressed in decimal and the default value is 162. The default number is assumed if this field is replaced with "default". All legal UDP port numbers are allowed. If the IP address is specified and this parameter is not specified, it is set to the default value.

Command example

```
Root> config snmp addV2target 1 xyz 192::2341:231:451 172
```

config.snmp.addV3Target

Syntax

```
addV3Target index [IP] [udpNum]
```

Description

This command configures the IP address and optionally the port number of a v3 trap recipient. The community name is not used for v3 Traps.

Parameters

This command has three parameters. The last one is optional.

index	The index of the target entry. Valid values are 1 to 6.
IP	The address of the trap recipient shown in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format).
udpNum	The UDP port number of the Trap recipient to which the SNMP agent sends the traps. This value is expressed in decimal and the default value is 162. The default number is assumed if this field is replaced with "default". All legal UDP port numbers are allowed. If this parameter is not specified, it is set to the default value.

Command example

```
Root> config snmp addV3target 2 182::221 172
```

config.snmp.authTraps

Syntax

```
authTraps enabledState
```

Description

This command enables or disables the authentication traps to be sent to the SNMP management stations when unauthorized stations try to access SNMP information from the director or switch.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of the authentication traps. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> config snmp authTraps enable

Root> config snmp authTraps 1
```

config.snmp.deleteAccessEntry

Syntax

```
deleteAccessEntry index
```

Description

This command deletes the specified entry from the access table.

Parameters

This command has one parameter:

commIndex	The index of the access entry. Valid values are 1 to 6.

Command example

```
Root> config snmp deleteAccessEntry 1
```

config.snmp.deleteCommunity

Syntax

```
deleteCommunity commIndex
```

Description

This command deletes an SNMP community and trap recipient, if configured.

Parameters

This command has one parameter:

commIndex	The community to be deleted. Valid values are integers in the range 1–6. This value was set in the commIndex parameter of the *config.snmp.addCommunity* command.

Command example

```
Root> config snmp deleteCommunity 5
```

config.snmp.deleteUserEntry

Syntax

```
deleteUserEntry index
```

Description

This command deletes the specified user entry from the user table.

Parameters

This command has one parameter:

index	The index of the user entry. Valid values are 1 to 6.

Command example

```
Root> config snmp deleteUserEntry 1
```

config.snmp.deleteTargetEntry

Syntax

```
deleteTargetEntry index
```

Description

This command deletes the specified entry from the target table.

Parameters

This command has one parameter:

Index	The index of the target entry. Valid values are 1 to 6.

Command example

```
Root> config snmp deletetargetentry 1
```

config.snmp.deleteV3Group

Syntax

```
deleteV3Group index
```

Description

This command deletes the specified entries from the Security-to-Group table.

Parameters

This command has one parameter:

index	The index of the user entry. Valid values are 1 to 6.

Command example

```
Root> config snmp deleteV3Group 1
```

config.snmp.sendTestTrap

Synopsis

```
sendTestTrap
```

Description

This command instantly generates the *fcConnUnitEvent* trap with an event type as “status” and event description as “Reason code 0”.

Parameters

This command has no parameters.

Command example

```
Root> config snmp sendTestTrap
```

config.snmp.setSNMPv3State

Syntax

```
setSNMPv3State enabledState
```

Description

This command enables/disables SNMPv3.

NOTE
If the SNMP User Table, Access Table, and Security-to-Group Tables are not properly configured, SNMP access is lost upon completion of this command. Use the command *config.snmp.validateUser* to ensure proper configuration of user entries.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of SNMPv3. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config snmp setSNMPv3State enable
```

config.snmp.setFaMibVersion

Syntax

```
setFaMibVersion versionNumber
```

Description

This command sets the version of the Fibre Alliance MIB with which the SNMP agent interacts. The version number can be set to 3.0 or 3.1.

Parameters

This command has one parameter:

versionNumber	The version of the Fibre Alliance MIB version number. Accepted values for this command are 3.0 or 3.1.

Command example

```
Root> config snmp setFaMibVersion 3.1
```

config.snmp.setState

Syntax

```
setState enabledState
```

Description

This command enables or disables the SNMP agent. When disabled, the SNMP agent does not respond to any requests or send any traps.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of the SNMP agent. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config snmp setState 1
```

config.snmp.show

Syntax

```
show
```

Description

This command shows the SNMP configuration of the switch.

Parameters

This command has no parameters.

Command example

```
Root> config snmp show
SNMP State:               Enabled
SNMPv3 State:             Disabled
FA MIB Version Number:    3.1
Authentication Traps:     Disabled

Index  Community Name   Write Auth       Trap Recipient         UDP Port
-----   ---------------  ----------      -------------------    --------
1         public           Enabled      2001::221:12              172
2         public1          Disabled     1001::121                 165
3         public5          Enabled      abc::291:1233             162
4         public3          Disabled     acd::1092:23              192
5         public12         Enabled      172.27.2.1                162
6         public2          Enabled      2001::c0e9:26f            182
```

Output

The switch configuration data is displayed as a table that includes the following properties:

SNMP Agent State	The state of the SNMP agent. If it is disabled, the SNMP agent does not respond to any requests and does not produce any traps.
FA MIB Version Number	The version of the Fibre Alliance MIB (FA MIB) that the SNMP agent is configured to use.
Authentication Traps	The state of the authentication traps (for example, *enabled*) that are sent to SNMP management stations when unauthorized stations attempt to access SNMP information from the switch.
Index	The community index number.
Community Name	The name of the community.
WriteAuth	The write authorization state.
Trap Recipient	The address of the trap recipient shown in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format).
UDP Port	The User Datagram Protocol (UDP) port number to which the switch sends traps for each recipient.

Output example

The output from the *config.snmp.show* command displays as follows:

```
SNMP Agent State:       Enabled
FA MIB Version Number:  3.0
Authentication Traps:   Enabled
Index  Community Name                 WriteAuth  Trap Recipient    UDP Port
-----  -----------------------------  ---------  ---------------   ------
1      CommunityName1                 Enabled    123.123.123.123   162
2      CommunityName2                 Enabled    10.25.25.10       144
3      CommunityName3                 Disabled   132.44.85.224     162
4      public                         Enabled                      162
5
6
```

config.snmp.showAccessTable

Syntax

```
showAccessTable [index]
```

Description

This command displays the configured values for the access table.

Parameters

This command has one optional parameter:

index	The index of the access entry. Valid values are 1 to 12.

Command example

```
Config.SNMP> showAccessTable
SNMPv3 State:    Enabled
Index  Group Name
-----  ----------
1      group1
2
3
4      v1Group
5
6
7      v2Group
8
9
10     usmGroup
11     usmGroup
12
```

or

If you specify the index, the output of this command will contain the following data:

Index	The index of the access entry. Valid values are 1 to 6.
Group Name	The group name.
Security Model	The security model.
Security Level	The security level.
Read View	The read view name.
Write View	The write view name.
Notify View	The notify view name.

```
Config.SNMP> showAccessTable 1
Index:              1
Security Model:     Any
Security Level:     None
Group Name:         group1
Read View:          fcmgmt_3_1
Write View:         fceos
Notify View:        internet
```

config.snmp.showTargetTable

Syntax

```
showTargetTable [index]
```

Description

This command displays the configured values for the target table.

Parameters

This command has one optional parameter:

index	The index of the access entry. Valid values are 1 to 6.

Command example

```
Root> config snmp showtargettable
SNMPv3 State:    Disabled

Index    Target IP             UDP Port   Community       MP Model
-----    ------------------  --------   -------------  --------
1         192::2341:231:451     172          xyz           SNMPv2
2         182::221              172                        SNMPv3
3
4
5
6
```

NOTE
The command “show.snmp.targetTable” on page 274 has functionality that is the same as this command.

config.snmp.showUserTable

Syntax

```
showUserTable
```

Description

This command displays the users configured presently in the USM table.

Parameters

This command has no parameters.

Output

This command displays the following switch configuration data:

SNMPv3 State	The state of SNMPv3.
Index	The index number.
Username	The user name.
Auth Protocol	The authentication protocol.
Privacy Protocol	The privacy protocol.

Command example

```
Config.SNMP> showUserTable

   SNMPv3 State:    Enabled
   Index  Username                          Auth Protocol      Privacy Protocol
   -----  --------------------------------  -----------------  ----------------
   1      User1                             No Authentication  No Privacy
   2      User2                             HMAC-MD5           No Privacy
   3      User3                             HMAC-SHA           DES
   4
   5
   6
```

NOTE
This command and the command "show.snmp.userTable" on page 276 has the same functionality.

config.snmp.showV3GroupTable

Syntax

```
showV3GroupTable
```

Description

This command displays the Security-to-Group table.

Parameters

This command has no parameters.

Output

This command displays the following switch configuration data:

SNMPv3 State	The state of SNMPv3.
Index	The index number.
Username	The user name.
Model	The security model.
Group Name	The group name.

Example

```
config.SNMP> showV3GroupTable
SNMPv3 State:    Enabled
    Index  Username                          Model  Group Name
    -----  --------------------------------  -----  ----------
    1      User1                             V1     Group1
    2
    3
    4
    5
    6
```

NOTE
This command and the command "show.snmp.V3GroupTable" on page 277 has the same functionality.

config.snmp.showViewTable

Syntax

```
showViewTable
```

Description

This command displays the values for the VACM views presently configured.

Parameters

This command has no parameters.

Output

This command displays the following switch configuration data:

View Name	The name of the view.
Type	The type of the view.
Object ID	The Object ID.

Command example

```
config.snmp> showViewTable

   View Name                       Type                Object ID
   ------------------------------  ------------------  ---------
   no_access                       View Excluded       .1.3.6.1
   internet                        View Included       .1.3.6.1
   management                      View Included       .1.3.6.1.2
   experimental                    View Included       .1.3.6.1.3
   private                         View Included       .1.3.6.1.4
   snmpv3                          View Included       .1.3.6.1.6
   fceos                           View Included       .1.3.6.1.4.1.289
   fcmgmt_3_1                      View Included       .1.3.6.1.2.1.8888
   fcmgmt_3_0                      View Included       .1.3.6.1.3.94
   fcfe                            View Included       .1.3.6.1.3.42
   system                          View Included       .1.3.6.1.2.1.1
   ip                              View Included       .1.3.6.1.2.1.4
```

config.snmp.validateUser

Syntax

```
validateUser username secModel secLevel
```

Description

This command searches the user, group, and access tables for the given username, security model, and security level. If the username, security model, and security level cannot be traced in these tables, a message is displayed with the reason.

Parameters

This command has three parameters:

username	The user name for the user validation.
secModel	The security model of the user.
secLevel	The security level of the user.

Output

This command displays the following switch configuration data:

Username	The user name.
Auth Protocol	The authentication protocol used for this user.
Priv Protocol	The privacy protocol used for this user.
Security Model	The security model for this user.
Security Level	The security level for this user.
Context Match	The context match method.
Group Name	The group that this user belongs to.
Read View	The read view access for this user.
Write View	The write view access for this user.
Notify View	The notify view access for this user.

Command example

```
Root> Config SNMP validateUser Jerry v1 noauthnopriv


Username:          Jerry
Auth Protocol:     No Authentication
Priv Protocol:     No Privacy
Security Model:    V1
Security Level:    No Authentication and No Privacy
Context Match:     Prefix
Group Name:        Group1
Read View:         internet
Write View:        management
Notify View:       private
```

config.switch

All commands under this branch operate on a particular switch attribute. Switch attributes are specific to the Fibre Channel switch nature of the product.

Some of the *config.switch* commands require that the switch be set offline. (Use the *maint.system.setOnlineState* to set the switch offline.) If some of these commands are entered while the switch is online, an error message results.

config.switch.apiState

Syntax

```
apiState apiEnabledState
```

Description

This command sets the state of the API interface. When disabled, access through the API interface is turned off.

Parameters

This command has one parameter:

apiEnabledState	The enabled/disabled state of the API interface. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config switch apiState enable
```

config.switch.banner

The banner command on the configuration branch enters the banner configuration branch. All commands operate on the banner content and the state of the banner.

This configured banner text is displayed during log in through CLI or EFCM Basic, if the banner state is enabled. Refer to *config.switch.banner.bannerText* for configuring the banner text.

For example, when you connect to the switch using the Telnet command:

```
McDATA (R) Fibre Channel Director Firmware Version 09.00.00
Access is restricted to Authorized personnel only
Username>
```

config.switch.banner.bannerText

Syntax

```
bannerText lineNumber lineContent
```

Description

This command configures the banner text for a particular line number.

Parameters

This command has two parameters:

lineNumber	The line number in the banner text. This can take a value from 0 to 24.
lineContent	The text for a particular line. If an empty line is to be displayed, an empty string in double quotation marks is to be configured. For a string that is separated by spaces, the entire string should be enclosed within quotation marks. This has an 80 character limitation and accepts alphanumeric characters.

Command example

```
config.switch.banner> bannerText 1 “McDATA (R) Fibre Channel Director Firmware
Version 08.00.00”

config.switch.banner> bannerText 2 “Access is restricted to Authorized personnel
only”

config.switch.banner> bannerText 3 “ ”
```

config.switch.banner.setCLIState

Syntax

```
setCLIState state
```

Description

This command configures the enabled state for whether the configured banner is displayed at the CLI login prompt.

Parameters

This command has one parameter.

state	The enabled/disabled state for CLI banner. This parameter can be set to *enable* or *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config switch banner setCLIState 1
```

config.switch.banner.setWebState

Syntax

```
setWebState state
```

Description

This command configures the enabled state for whether the configured banner is displayed at the Web login.

Parameters

This command has one parameter.

state	The enabled/disabled state for CLI banner. This parameter can be set to *enable* or *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config switch banner setWebState 0
```

config.switch.banner.show

Syntax

```
show
```

Description

This command displays the configured banner.

Parameters

This command has no parameters.

Command example

```
Root> config switch banner show
```

Output

The login banner and settings are displayed on the screen.

Output example

```
Config.Switch> banner
Config.switch.banner> show
```

```
CLI Banner Enabled State:    Disabled
Web Banner Enabled State:    Disabled
Banner content:
McDATA (R) Fibre Channel Director Firmware Version 09.00.00
Access is restricted to Authorized personnel only
config.switch.banner>
```

config switch blockDupWWN

Syntax:

```
blockDupWWN option
```

Description

This command avoids logging of two devices at the same port WWN in a fabric. When a second device tries to log in with the same port WWN switch, the blockDupWWN command blocks the device and displays the message “Blocked due to duplicate WWN”. If blockDupWWN is disabled, then two devices are allowed to log in with the same port WWN

Parameters

Option	1 – Enable feature. 0 - Disable the feature. Default Value: 0 – disable

Command example

```
Root> config switch blockDupWWN 1
```

config.switch.domainIDOffset

Syntax

```
domainIDOffset offset
```

Description

This command configures the offset of the Domain ID range in which the switch or director should operate.

Parameters

This command has one parameter:

offset	The Domain ID offset. Values are in hexadecimal. Valid values are: *00* *32* *64* *96* *128* *160* *192*

Command example

```
Root> config switch domainIDOffset 160
```

config.switch.domainRSCN

Syntax

```
domainRSCN domainRSCNState
```

Description

This command sets the domain RSCN state for the switch or director. You can run this command when the switch or director is either offline or online. When this parameter is enabled, domain registered state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices.

As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

Parameters

This command has one parameter:

domainRSCNState	The enabled/disabled state of the domain RSCN. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config switch domainRSCN 1
```

config.switch.edTOV

Syntax

```
edTOV timeoutValue
```

Description

This command sets the error detect timeout value (E_D_TOV) for the switch.

NOTE
The switch must be set offline before this command is entered.

Special care should be used when scripting this command due to its relationship with R_A_TOV.

Parameters

This command has one parameter:

timeoutValue	The new E_D_TOV value. The units for this value are tenths of a second. This parameter must be an integer in the range 2–600 (0.2 second to 60 seconds), and it must be smaller than the R_A_TOV.

Command example

```
Root> config switch edTOV 4
```

config.switch.haMode

Syntax

```
haMode haEnabledState
```

Description

This command sets the state of high availability.

Parameters

This command has one parameter:

haEnabledState	The enabled/disabled state of high availability. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config switch haMode enable
```

NOTE
This command is applicable only to Sphereon 4400.

config.switch.insistDomainId

Syntax

```
insistDomainId insistentDomainIdState
```

Description

This command sets the insistent domain ID state for the switch.

Parameters

This command has one parameter:

insistentDomainIdState	The enabled/disabled state of the insistent domain ID. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config switch insistDomainId 1
```

NOTE
The Insistent Domain ID must be enabled if the Enterprise Fabric Mode (an optional SANtegrity feature) or Preferred Path is enabled.

config.switch.interopMode

Syntax

```
interopMode interopMode
```

Description

This command sets the interoperability mode for the switch. The switch must be offline to complete this command.

NOTE
The switch must be set offline before this command is entered.

Parameters

This command has one parameter:

interopMode	The interoperability mode. Valid values are *mcdata* and *open*: *mcdata* — McDATA Fabric 1.0. Select this mode if the fabric contains only supported switches and directors that are also operating in McDATA Fabric 1.0 mode. *open* — Open Fabric 1.0. Select this mode if the fabric contains supported switches and directors and other Open Fabric-compliant switches. Select this mode for managing heterogeneous fabrics.

Command example

```
Root> config switch interopMode open
```

config.switch.islFSPFCost

Syntax

```
islFSPFCost islFSPFCostState
```

Description

This command configures the Fabric Shortest Path First (FSPF) cost of Inter-Switch Links (ISLs) on the switch. Cost is used to determine the shortest path (or the path which would take the least amount of time for traffic to travel) to a destination.

Parameters

This command has two parameters:

ignore	Every ISL has the same FSPF cost. In essence, the actual FSPF cost is ignored.
port	Each ISL has a McDATA default cost, which depends on the speed of the port.

NOTE
It is recommended that all the switches in the fabric have the same value for the ISL FSPF Cost Configuration parameter.

Command example

```
Root> config switch islFSPFCost ignore
```

config.switch.ltdFabRSCN

Syntax

```
ltdFabRSCN ltdFabRSCNState
```

Description

This command sets the status of limited fabric RSCNs. When enabled, fabric registered state change notifications (RSCNs) are suppressed during an IPL.

Parameters

This command has one parameter:

ltdFabRSCNState	The enabled/disabled state of the limited fabric RSCN state. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config switch ltdFabRSCN 1
```

config.switch.prefDomainId

Syntax

```
prefDomainId domainId
```

Description

This command sets the preferred domain ID for the switch or director. The switch or director must be offline to complete this command.

Parameters

This command has one parameter:

domainId	The new preferred domain ID value. This parameter must be an integer in the range 1–31.

Command example

```
Root> config switch prefDomainId 1
```

config.switch.priority

Syntax

```
priority Priority
```

Description

This command sets the switch priority.

NOTE
The switch must be set offline before this command is entered.

Parameters

This command has one parameter:

Priority	The switch priority. Valid values are: *principal*, *default*, or *neverprincipal*. *principal* — sets the numerical switch priority to 1. The switch with a priority of 1 becomes the principal switch; however, if two or more switches have a priority of 1, the switch with the lowest WWN becomes the principal switch. *default* — sets the numerical switch priority to 254. If no switch is set to principal, the switch with a priority 254 becomes the principal switch; however, if two or more switches have a priority of 254, the switch with the lowest WWN becomes the principal switch. *neverprincipal* — sets the numerical switch priority to 255. This disables the switch from becoming a principal switch. At least one switch in a multiswitch fabric must have a switch priority value of *principal* or *default*. The number codes 2–253 are not in use now.

Command example

```
Root> config switch priority principal
```

config.switch.raTOV

Syntax

```
raTOV timeoutValue
```

Description

This command sets the resource allocation timeout value (R_A_TOV) for the switch.

NOTE
The switch must be set offline before this command is entered.

Special care should be taken when scripting this command due to its relationship with E_D_TOV.

Parameters

This command has one parameter:

timeoutValue	The new R_A_TOV value. The units for this value are tenths of a second. This parameter must be an integer in the range 10–1200 (1 second to 120 seconds), and it must be greater than the E_D_TOV.

Command example

```
Root> config switch raTOV 20
```

config.switch.rerouteDelay

Syntax

```
rerouteDelay rerouteDelayState
```

Description

This command enables or disables the rerouting delay for the switch.

NOTE
The switch can be either offline or online when this command is executed.

This command is only applicable if the configured switch is in a multiswitch fabric. Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination.

If there is a change in the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order because frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the *config.switch.edTOV* command. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path. Note that during this delay period, frames addressed to the destinations that are being rerouted are discarded if they are Class 3 frames and rejected if they are Class 2 or Class F frames.

Parameter

This command has one parameter:

rerouteDelayState	The enabled/disabled state of rerouting delay. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> config switch rerouteDelay true
```

config.switch.RSCNZoneIsolation

Syntax

```
RSCNZoneIsolation RSCNZoneIsolationState
```

Description

This command configures the state of RSCN Zone Isolation.

Parameters

This command has one parameter:

RSCNZoneIsolationState	The enabled/disabled state of RSCN Zone Isolation. Valid values are *fabric* and *none*. When set to *fabric*, RSCNs are only sent to affected fabric members when zoning information changes. When set to *none*, filtering of RSCNs do not take place, and RSCNs are sent to all zoneset members when zoning information changes.

config.switch.safeZoning

Syntax

```
safeZoning safeZoningState
```

Description

This command sets the state for safe zoning. When enabled, zone merges do not take place unless zone sets are equivalent; in addition, the option to set the default zone is disabled.

Parameters

This command has one parameter:

safeZoningState	The enabled/disabled state of safe zoning. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config switch safeZoning enable
```

config.switch.setipv6

Syntax

```
setIPv6 <state>
```

Description

This command sets the enabled state of the IPv6 feature.

Parameters

This command has one parameter:

State	enable/disable the state of IPv6

Command example

```
Root> config switch setipv6 1
```

config.switch.speed

Syntax

```
speed switchSpeed
```

Description

This command sets the speed for the switch.

NOTE
This command is only applicable to the Intrepid 6064.

NOTE
The switch must be set offline before this command is entered.

A switch can be configured to operate at 1 Gbps or 2 Gbps.

If the switch has FPM cards, configuring the switch speed to 2 Gbps makes all the ports on the FPM cards inactive, and their operational state is set to inactive. FPM ports do not support 2 Gbps and, therefore, remain inactive after the switch is returned to the online state.

Parameters

This command has one required parameter.

switchSpeed	The speed of the switch. Valid values are *1 Gb/sec* and *2 Gb/sec*.

Command Examples

```
Root> config switch speed 2g
```

config.switch.show

Syntax

```
show
```

Description

This command displays the switch configuration.

NOTE
The switch can be either offline or online when this command is executed.

Parameters

This command has no parameters.

Command example

```
Root> config switch show
```

Output

The switch configuration data is displayed as a table that includes the following properties:

R_A_TOV	The Resource Allocation Time Out Value. This time outs the operations that depend on the maximum possible time that a frame can be delayed in a fabric and still be delivered.
E_D_TOV	The Error Detect Time Out Value. This indicates the maximum turnaround time that an operation could require.
Preferred Domain ID	The preferred domain ID of the switch.
Switch Priority	The switch priority. Values are *Principal is 1*, *Default is 2 to 254*, or *Never Principal is 255*.
Speed	The switch speed. (This is available only for intrepid 6064)
Rerouting Delay	The rerouting delay that ensures that frames are delivered in order through the fabric to their destination. Values are *Enabled* or *Disabled*.
Interop Mode	The interoperability mode for the switch.
Insistent Domain Id	When enabled, this ensures that the embedded firmware cannot change the preferred domain ID of a switch.
Domain RSCN	When enabled, this allows domain RSCNs to be sent to registered members of the fabric.

Zoning RSCN	When enabled, allows zoning RSCNs to be sent to registered members of the fabric.
Limited Fabric RSCN	When enabled, fabric RSCNs are suppressed after an IPL.
Zone FlexPars	When set to *fabric*, RSCNs are only sent to affected fabric members when zoning information changes. When set to *none*, filtering of RSCNs do not take place, and RSCNs are sent to all zoneset members when zoning information changes.
RSCN Zone Isolation	When set to *fabric*, RSCNs are only sent to affected fabric members when zoning information changes. When set to *none*, filtering of RSCNs do not take place, and RSCNs are sent to all zoneset members when zoning information changes.
Safe Zoning	The Safe Zoning State.
ISL FSPF Cost	The method for computing the FSPF cost for ISLs.
Web Enable	The enabled state of web.
API Enable	The API enable state.
HA Mode	The enabled state of high availability mode.
Domain ID offset	This configures Domain ID offset.
PassExpirationDays	The password expiration time in days for the management users.

Output example

The output from the *config.switch.show command* displays as follows:

```
R_A_TOV:                100
E_D_TOV:                20
Preferred Domain ID:    1
Domain ID Offset:       96
Switch Priority:        Default
Speed:                  2 Gb/sec
Rerouting Delay:        Disabled
Interop Mode:           McDATA Fabric 1.0
Insistent Domain ID:    Enabled
Domain RSCN:            Enabled
Zoning RSCN:            Enabled
Limited Fabric RSCN:    Disabled
Zone FlexPars:          No Filtering
RSCN Zone Isolation:    No Filtering
Safe Zoning:            Disabled
ISL FSPF Cost:          By Port Speed
Web Enabled:            Enabled
API Enabled:            Enabled
Password Exp. Time:     0
```

config.switch.webState

Syntax

```
webState webEnabledState
```

Description

This command sets the state of the web interface. When disabled, access through the web interface is turned off.

Parameters

This command has one parameter:

webEnabledState	The enabled/disabled state of the web interface. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config switch webState enable
```

config.switch.zoneFlexPars

Syntax

```
zoneFlexPars zoneFlexParstate
```

Description

This command configures the state of Zone FlexPars.

Parameters

This command has one parameter:

zoneFlexParsState	The enabled/disabled state of Zone FlexPars. Valid values are *fabric* and *none*. When set to *fabric*, RSCNs are only sent to affected fabric members when zoning information changes. When set to *none*, filtering of RSCNs do not take place, and RSCNs are sent to all zoneset members when zoning information changes.

Command example

```
Root> config switch zoneFlexPars fabric
```

config.switch.zoningRSCN

Syntax

```
zoningRSCN  zoningRSCNState
```

Description

This command sets the state of Zoning RSCNs.

Parameters

This command has one parameter:

zoningRSCNState	The enabled/disabled state of Zoning RSCNs. Valid values are *enable*, *disable*, *true*, and *false*. Boolean 1 and 0 values may also be substituted.

config.syslog

The syslog feature records events such as log-ins, configuration changes, and error messages that occur on the switch. If an error condition occurs, the switch attempts to write an entry to the system log. The syslog feature sends the user requested logs (supported logs) to the syslog service on a remote host.

You may configure up to three remote syslog recipients. A single facility may be configured for each remote syslog recipient and the default is *Local 0*. All syslog facilities are limited to the *local use* facility (Local 0 - Local 7).

config.syslog.addServer

Syntax

```
addServer index IP facility
```

Description

This command configures a syslog server at a given index.

Parameters

This command has three parameters:

index	The index number for the server. Possible values are 1 to 3.
IP	The IP address of the server.(either in V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format)).
facility	The facility for the server. Possible values are *Local0 - Local7.*

Command example

```
Root> config syslog addserver 2 2003::331:241:244 local1
```

config.syslog.deleteServer

Syntax

```
deleteServer index
```

Description

This command deletes a syslog server configuration.

Parameters

This command has one parameter:

index	The index number of the server to be deleted. Possible values are 1 to 3.

Command example

```
Root> config syslog deleteserver 2
```

config.syslog.setLogConfig

Syntax

```
setLogConfig logName state
```

Description

This command enables syslog support for the given log.

Parameters

This command has two parameters:

logName	The log type. Possible values are *Event, Trunking, Link, Security, Audit, Fabric, and Frame.*
state	The enabled/disabled state of syslog. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted. If the state is enabled, messages for that log is sent to the configured syslog servers.

Command example

```
Root> config syslog setLogConfig event enable
```

config.syslog.setState

Syntax

```
setState enabledState
```

Description

This command sets the enabled or disabled state for the syslog feature.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of the syslog feature. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> config syslog setState enable
```

config.syslog.show

Syntax

```
show
```

Description

This command displays the syslog configuration.

NOTE
The command "show.syslog" on page 284 has functionality that is the same as this command.

Parameters

This command has no parameters.

Output

The syslog configuration is shown as a table of properties. The following properties are displayed:

Log	The index number of the server.
State	The enabled/disabled state of syslog support.
Index	The index number of the server.
IP Address	The IP address of the server.(either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format)).
Facility	The facility level for the server. Values are *Local 0 - Local 7*.

Command example

```
Root> config syslog show
Syslog State:    Disabled

Index  IP Address             Facility
-----    ------------------   --------
1        2001::11               local0
2        2003::331:241:244      local1
3
```

With the system command, the configuration branch enters the system configuration branch. All commands under this branch operate on a particular system attribute. System attributes are generic attributes that are not specific to Fibre Channel, and thus would be present on any product.

config.system.contact

Syntax

```
contact systemContact
```

Description

This command sets the system contact attribute.

Parameters

This command has one parameter:

systemContact	The new system contact string for the director or switch. The contact can contain 0–255 characters.

Command example

```
Root> config system contact Joe
```

config.system.date

Syntax

```
date systemDate systemTime
```

Description

This command sets the system date and time.

Parameters

This command has two required parameters:

systemDate	The new system date. The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. Valid date values include: mm: 1–12 dd: 1–31 yyyy: >1980
systemTime	The new system time. The format of the time parameter must be hh:mm:ss. Valid time values include: hh: 0–23 mm: 0–59 ss: 0–59

Command examples

```
Root> config system date 04:16:2001 10:34:01

Root> config system date 10/09/2001 14:07:55
```

config.system.description

Syntax

```
description systemDescription
```

Description

This command sets the system description string.

Parameters

This command has one parameter:

systemDescription	The new system description string for the director or switch. The name can contain 0–255 characters.

Command example

```
Root> config system description McDATAIntrepid6140FibreChannelDirector
```

config.system.location

Syntax

```
location systemLocation
```

Description

This command sets the system location attribute.

Parameters

This command has one parameter:

systemLocation	The new system location for the director or switch. The location can contain 0–255 characters.

Command example

```
Root> config system location Everywhere
```

config.system.name

Syntax

```
name systemName
```

Description

This command sets the system name attribute.

Parameters

This command has one required parameter:

systemName	The new system name for the switch or switch. The name can contain 0–24 characters.

Command example

```
Root> config system name JoeSwitch
```

config.system.show

Syntax

```
show
```

Description

This command shows the system configuration.

Parameters

This command has no parameters.

Command example

```
Root> config system show
```

Output

The system configuration is displayed as a table that includes the following properties:

Name	The system name.
Description	The system description.
Contact	The system contact.
Location	The system location.
Date/Time	The system date and time.

Output examples

The output from the *config.system.show* command displays as follows:

```
Name:         Joe's Switch
Description:  McDATA Intrepid 6140 Fibre Channel Director
Contact:      Joe
Location:     Everywhere
Date/Time:    04/16/2001  10:34:01
```

config.tunnel.add

Syntax

```
addParams <index> <localip> <remoteip> <hoplimit> <status>
```

Description

This command configures a new tunnel entry for the tunnel interface.

Parameters

Index	The index of the tunnel entry. Valid values are 0-2.
Localip	Local ip address should represent in 4 byte dotted-decimal format.
Remoteip	Remote ip address should represent in 4 byte dotted-decimal format.
Hoplimit	valid the integer values up to 255.
Status	enable/disable the state of tunnel.

Command example

```
Root> config tunnel add 1 12.2.21.1 13.5.6.11 231 1
```

config.tunnel.delete

Syntax

```
delete <index>
```

Description

This command removes the tunnel entry from the tunnel interface.

Parameters

Index	The index of the tunnel entry. Valid values are 0-2.

Command example

```
Root> config tunnel delete 1
```

config.tunnel.edit

Syntax

```
addParams <index> <localip> <remoteip> <hoplimit> <status>
```

Description

This command edits the configured tunnel interface.

Parameters

Index	The index of the tunnel entry. Valid values are 0-2.
Localip	Local ip address should represent in 4 byte dotted-decimal format.
Remoteip	Remote ip address should represent in 4 byte dotted-decimal format.
Hoplimit	valid the integer values up to 255.
Status	enable/disable the state of tunnel.

Command Example

```
Config> tunnel edit 0 172.26.22.25 172.26.22.28 1 1
```

config.tunnelroute.edit

Syntax

```
addParams <tunnel_index> <tunnel_routeindex> <routeip> <prefix>
```

Description

This command edits the configured tunnelroute for tunnel interface.

Parameters

tunnel_index	The index of the tunnel entry. Valid values are 0-2
tunnel_routeindex	The index of the tunnelroute entry. Valid values are 0-2
Routeip	Route IP address either V6 format or V4 format.
Prefix	validate the integer value from 4-128

Command Example

```
Config> tunnelroute edit 0 0 2520::22 64
```

config.tunnel.show

Syntax

```
show <tunnel_index>
```

Description

This command displays the configured tunnel entries.

Parameters

Index	The index of the tunnel entry. Valid values are 0-2.

Command example

```
Root> config tunnel show
```

Output examples

The output from the *config.tunnel.show* command displays as follows:

```
   Index   Local IP             Remote IP     Hop limit   status
   ------  -------------------  -----------   ---------   ----------
   0       12.2.2.1              1.2.4.6        123          1
   1       12.3.55.77           1.2.23.3        91           0
   2       112.3.55.77         11.2.23.13       111          1
```

config.tunnelroute.add

Syntax

```
addParams <tunnel_index> <tunnel_routeindex> <routeip> <prefix>
```

Description

This command configures a new tunnel route entry of the specified tunnel index.

Parameters

tunnel_index	The index of the tunnel entry. Valid values are 0-2
tunnel_routeindex	The index of the tunnelroute entry. Valid values are 0-2
Routeip	Route IP address either V6 format or V4 format.
Prefix	validate the integer value from 4-128

Command example

```
config tunnelroute add 0 0 2002::22 123
```

config.tunnelroute.delete

Syntax

```
delete <tunnel_index> <tunnel_routeindex>
```

Description

This command removes the tunnel route entry of the specified tunnel index.

Parameters

tunnel_index	The index of the tunnel entry. Valid values are 0-2
tunnel_routeindex	The index of the tunnelroute entry. Valid values are 0-4

Command example

```
config tunnelroute delete 0 1
```

config.tunnelroute.show

Syntax

```
<tunnel_index>
```

Description

This command displays the configured tunnel route entries of the specified tunnel entry.

Parameters

tunnel_index	The index of the tunnel entry. Valid values are 0-2

Command example

```
Root> Config tunnelRoute show 0
```

Output examples

The output from the *config.tunnelroute.show* command displays as follows:

```
Index   Route IP                  Prefix
------  -------------------      ---------
0       2001::11                    12
1       2011::111                  121
2       400:222::23                102
```

config.zoning

Note that the *config.zoning* commands function in a different way from most CLI commands, which are single action commands that take effect immediately. A zoning configuration is typically too complicated to be described by a single command, so the first zoning command entered invokes a work-area editor. The commands take effect on a temporary copy of a zone set in the work area until the temporary copy in the work area is activated to the fabric--or is discarded.

Because not all the verification of the zone set can occur on the temporary copy in the work area, it is possible, however unlikely, that the copy of the zone set encounters no errors until the zone set is activated to the fabric.

NOTE
Port numbers cannot be used for zone members if the interoperability mode for the switch or director is set to Open Fabric 1.0 mode. In this case, you must use port WWNs as zone members.

NOTE
A Sphereon 4300 Switch cannot participate in a fabric unless the Fabric Capable feature is enabled. For more information, see the *Sphereon 4300 Switch Installation and Service Manual* (620-000171).

Table 4 shows the limits for configuring zoning in McDATA fabrics that are supported by switch and director firmware as of 11/14/03. Although EFCM 8.0 or EFCM 8.0b may allow you to configure greater values in the Zoning Library, values in this table have been tested and are supported. For the latest limits, refer to the *Supported Fabrics Configuration Document* located on www.brocade.com or contact your customer support representative.

TABLE 4 Supported Zoning Configurations

Product	Intrepid 6064 Intrepid 6140	Sphereon 4700	Sphereon 4400	Sphereon 4500	Sphereon 4300	Sphereon 3x32 Sphereon 3x16	ED-5000
Number of End Ports	1024	1024	1024	1024	1024	1024	1024
Unique Zone Members	4096	4096	4096	4096	4096	4096	1042
Members per Zone	4096	4096	4096	4096	4096	4096	1024
Zones	2048	2048	2048	2048	2048	2048	512

config.zoning.activateZoneSet

Syntax

```
activateZoneSet
```

Description

This command activates the zone set contained in the work area to the fabric and takes effect immediately.

Parameters

This command has no parameters.

Command example

```
Root> config zoning activateZoneSet
```

NOTE
If the interoperability mode for the switch or director is set to Open Fabric 1.0 mode when the zone is activated, any zone members specified by the port number are ignored.

config.zoning.addPortMem

Syntax

```
addPortMem "zoneName" domainId portNumber
```

Description

This command adds the domain ID and port number of a zone member to the specified zone in the work area.

NOTE
Port numbers cannot be used for zone members if the interoperability mode for the switch or director is set to Open Fabric 1.0 mode.

NOTE
A product can have a maximum of 4096 zone members in its zones.

NOTE
The ED-5000 supports a maximum of 512 zones.

Parameters

This command has the following parameters:

zoneName	The name of the zone.
domainId	The domain ID of the member to be added to the zone. Valid values are in the range 1–31.
portNumber	The port number of the member to be added to the zone. Valid port number values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> config zoning addPortMem TheUltimateZone 10 6
```

config.zoning.addWwnMem

Syntax

```
addWwnMem zoneName wwn
```

Description

This command adds a WWN zone member to the specified zone in the work area.

NOTE
A product can have at most 4096 zone members in its zones.

NOTE
The ED-5000 supports a maximum of 512 zones.

Parameters

This command has two parameters:

zoneName	The name of the zone.
wwn	The WWN of the member to be added to the zone. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).

Command example

```
Root> config zoning addWwnMem TheUltimateZone 10:00:00:00:C9:22:9B:64
```

config.zoning.addZone

Syntax

```
addZone zoneName
```

Description

This command adds a new (empty) zone to the zone set in the work area.

NOTE
Changes are not activated on the switch until the *config.zoning.activateZoneSet* command is issued.

NOTE
A zone set can have a maximum of 4096 unique zone members.

NOTE
A switch or director can have a maximum of 2048 zones in a zone set, except for the ED-5000, which allows a maximum of 512 zones.

Parameters

This command has one parameter:

zoneName	The name of the new zone. The zoneName must contain 1–64 characters. Valid characters are: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789$-^_ Spaces are not permitted, and the first character must be alphabetical.

Command example

```
Root> config zoning addZone TheUltimateZone
```

config.zoning.clearZone

Syntax

```
clearZone zoneName
```

Description

This command clears all zone members for the specified zone in the work area. This command does not change the zone name.

Parameters

This command has one parameter:

zoneName	The name of the zone to be cleared.

Command example

```
Root> config zoning clearZone TheNotUltimateAtAllZone
```

config.zoning.clearZoneSet

Syntax

```
clearZoneSet
```

Description

This command clears the zone set contained in the work area, removing all zones, and takes effect immediately. This command does not change the zone set name.

Parameters

This command has no parameters.

Command example

```
Root> config zoning clearZoneSet
```

config.zoning.deactivateZoneSet

Syntax

```
deactivateZoneSet
```

Description

This command places all attached devices in the default zone and takes effect immediately for the entire fabric. This command clears both the active zone set and the working area. This command takes effect immediately in the fabric.

NOTE
The default zone must be activated independently of this command.

Parameters

This command has no parameters.

Command example

```
Root> config zoning deactiveZoneSet
```

config.zoning.deletePortMem

Syntax

```
deletePortMem zoneName domainId portNumber
```

Description

This command deletes a domain ID and port number for a zone member in the specified zone in the work area.

Parameters

This command has three parameters:

zoneName	The name of the zone that contains the member to be deleted.
domainId	The domain ID of the member that has to be deleted from the zone. Valid domain IDs are in the range 1–31.
portNumber	The port number of the member to be deleted from the zone. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> config zoning deletePortMem TheUltimateZone 10 5
```

config.zoning.deleteWwnMem

Syntax

```
deleteWwnMem zoneName wwn
```

Description

This command removes a WWN member from a zone that is in the work area.

Parameters

This command has two parameters:

zoneName	The name of the zone that contains the member to be deleted.
wwn	The WWN of the member to be deleted from the zone. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).

Command example

```
Root> config zoning deleteWwnMem TheNotSoUltimateZone 10:00:00:00:C9:22:9B:AB
```

config.zoning.deleteZone

Syntax

```
deleteZone zoneName
```

Description

This command deletes a zone from the zone set in the work area.

NOTE
Changes are not activated on the switch until the *config.zoning.activateZoneSet* command is issued.

Parameters

This command has one parameter:

zoneName	The name of the zone to be deleted.

Command example

```
Root> config zoning deleteZone TheLeastUltimateZone
```

config.zoning.disableSplZoneSet

Syntax

```
disableSplZoneSet
```

Description

This command deletes the RD zones in the zone set.

NOTE
This command works, when the switch is not in a multiple switch fabric. To run this command remove the switch from the fabric and delete the Special zones and replace in the fabric.

Parameters

This command has no parameters

Command example

```
Root> config zoning disableSplZoneSet
```

NOTE
This command either displays a error message or nothing(blank). Nothing indicates that the command configured successfully.

config.zoning.renameZone

Syntax

```
renameZone oldZoneName newZoneName
```

Description

This command renames a zone in the work area.

Parameters

This command has two parameters:

oldZoneName	The current zone name of the zone to be renamed.
newZoneName	The new zone name. The newZoneName must contain 1–64 characters. Valid characters are: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789$-^_ Spaces are not permitted, and the first character must be alphabetical.

Command example

```
Root> config zoning renameZone TheOldUltimateZone TheUltimateZone
```

config.zoning.renameZoneSet

Syntax

```
renameZoneSet zoneSetName
```

Description

This command changes the name of the zone set in the work area.

NOTE
Changes are not activated on the switch until the *config.zoning.activateZoneSet* command is issued.

Parameters

This command has one parameter:

zoneSetName	The new name for the zone set. The zoneSetName must contain 1–64 characters. Valid characters are: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789$-^_ Spaces are not permitted, and the first character must be alphabetical.

Command example

```
Root> config zoning renameZoneSet TheUltimateZoneSet
```

config.zoning.replaceZoneSet

Syntax

```
replaceZoneSet
```

Description

This command replaces the work area with the active zone set that is currently loaded on the fabric.

Parameters

This command has no parameters.

Command example

```
Root> config zoning replaceZoneSet
```

config.zoning.setDefZoneState

Syntax

```
setDefZoneState defaultZoneState
```

Description

This command enables or disables the default zone and takes effect immediately fabric wide.

NOTE
This command takes effect immediately in the fabric.

Parameters

This command has one parameter:

defaultZoneState	The enabled/disabled state of the default zone. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> config zoning setDefZoneState false

Root> config zoning setDefZoneState 0
```

config.zoning.showActive

Syntax

```
showActive
```

Description

This command shows the zoning configuration saved on the fabric.

Parameters

This command has no parameters.

Command example

```
Root> config zoning showActive
```

Output

The zoning configuration data is displayed as a table that includes the following properties.

Active ZoneSet	The enabled status, name, and member zones of the zone set.

Output example

The output from the *config.zoning.showActive* command displays as follows:

```
Active Zone Set
Default Zone Enabled:  False
ZoneSet:  TheUltimateZoneSet
    Zone:  TheUltimateZone
           ZoneMember: Domain 10, Port 6
           ZoneMember: Domain 15, Port 2
           ZoneMember: Domain 2, Port 63
           ZoneMember: 10:00:00:00:C9:22:9B:64
           ZoneMember: 10:00:00:00:C9:22:9B:BD
    Zone:  TheNotSoUltimateZone
           ZoneMember: 10:00:00:00:C9:22:9B:AB
           ZoneMember: 10:00:00:00:C9:22:9B:C6
           ZoneMember: 10:00:00:00:C9:22:9B:AB
    Zone:  TheNotUltimateAtAllZone
           ZoneMember: Domain 2, Port 63
```

config.zoning.showPending

Syntax

```
showPending
```

Description

This command shows the zoning configuration in the work area of the zone set that has not yet been activated.

Parameters

This command has no parameters.

Command example

```
Root> config zoning showPending
```

Output

The zoning configuration data is displayed as a table that includes the following properties:

Local ZoneSet	The enabled status, name, and member zones of the zone set.

Output example

The output from the *config.zoning.showPending* command displays as follows:

```
Pending Zone Set
Default Zone Enabled:  False
ZoneSet:  TheNewUltimateZoneSet
    Zone:  TheNewUltimateZone
           ZoneMember: Domain 10, Port 6
           ZoneMember: Domain 15, Port 2
    Zone:  TheNewNotSoUltimateZone
           ZoneMember: 10:00:00:00:C9:22:9B:AB
           ZoneMember: 10:00:00:00:C9:22:9B:C6
           ZoneMember: 10:00:00:00:C9:22:9B:AB
    Zone:  TheNewNotUltimateAtAllZone
          ZoneMember: Domain 2, Port 63
```

config.zoning.showActiveSpl

Syntax

```
showActiveSpl
```

Description

This command displays the active special zones in the zone set.

Parameters

This command has no parameters.

Command example

```
Root>config zoning showActiveSpl
```

Output

```
Redirect_ZoneSet: eeeee
    Zone: red_0917_test
        Zone Member: 10:00:00:00:C9:3B:45:A0
        Zone Member: 10:00:00:00:C9:39:83:D3
        Zone Member: 10:00:00:00:C9:39:83:D4
        Zone Member: 10:00:00:00:C9:3B:45:A1
```

config.zoning.showSplZoneState

Syntax

```
showSplZoneState
```

Description

This command verifies the whether the special zones are activated are not and ‘True’ indicates that the special zone is activated.

Parameters

This command has no parameters.

Command example

```
Root>config zoning showSplZoneState
```

Output

```
Special_Zone Flag: True
Special_Zone Checksum: 18624
```

maint

The maint branch of the CLI command tree contains commands that relate to maintenance activities. The commands in the maint branch can be used only by the administrator.

ATTENTION
Note that the *maint.system.resetConfig* command resets all configuration data and non-volatile settings, including network information, to their default values (factory settings). Management access may be lost until the network information is restored.

maint.port.beacon

Syntax

```
beacon portNumber beaconState
```

Description

This command enables or disables port beaconing for a port.

Parameters

This command has two required parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 4700 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
beaconState	The enabled/disabled state of beaconing. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> maint port beacon 4 false

Root> maint port beacon 4 0
```

maint.port.reset

Syntax

```
reset portNumber
```

Description

This command resets an individual port without affecting any other ports. However, if a device is attached to the port and the device is online, the reset causes a link reset to occur. If the port is in a failed state (that is, after failing a loopback test), the reset restores the port to an operational state. The reset also clears all statistics counters and disables port beaconing for the specified port.

Parameters

This command has one parameter:

portNumber	The port number to be reset. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> maint port reset 4
```

maint.system.beacon

Syntax

```
beacon beaconState
```

Description

This command enables or disables unit beaconing.

Parameters

This command has one parameter:

beaconState	The enabled/disabled state of unit beaconing. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> maint system beacon false
```

```
Root> maint system beacon 0
```

maint.system.clearSysError

Syntax

```
clearSysError
```

Description

This command clears the system error light.

Parameters

This command has no parameters.

Command example

```
Root> maint system clearSysError
```

maint.system.ipl

Syntax

```
ipl
```

Description

This command performs an IPL on the switch.

NOTE
Connection to the CLI is lost when this command runs.

Parameters

This command has no parameters.

Command example

```
Root> maint system ipl
```

maint.system.resetConfig

Syntax

```
resetConfig
```

Description

This command resets all NVRAM configuration parameters to their default values, including feature keys and IP addresses.

NOTE
This command performs an IPL on the switch. Connection from the CLI to the switch is lost when this command runs.

NOTE
This command resets all configuration data and nonvolatile settings, including network information, to their default values (factory settings). Management access may be lost until the network information is restored.

The default values are set in the firmware of the director or switch. For information about the default values, refer to the service manual of your director or switch.

Parameters

This command has no parameters.

Command example

```
Root> maint system resetConfig
```

maint.system.setOnlineState

Syntax

```
setOnlineState onlineState
```

Description

This command sets the switch online or offline.

Parameters

This command has one parameter:

onlineState	The online/offline state of the switch. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command examples

```
Root> maint system setOnlineState true

Root> maint system setOnlineState 1
```

perf

The perf branch of the CLI command tree contains commands that relate to performance services. The commands in the perf branch can be used by either the administrator or the operator.

The counters in perf command output are 32-bit values that wrap at 4,294,967,296. To calculate the full value of a counter, multiply 4,294,967,296 by the value in the wrap field, and add the resulting product to the value in the count field. For example, if a TxFrames statistic has a count value of 1842953 and a wrap value of 12, the full value of the counter is:

(4,294,967,296 x 12) + 1842953 = 51,541,450,505.

perf.AFD

The Advanced Fabric Diagnostics (AFD) command on the performance branch enters the AFD configuration branch. All commands under this branch operate on a particular feature of fabric diagnostics.

perf.AFD.HDDReport

Syntax

```
HDDReport logSetting
```

Description

This command configures the Hot Device Detection (HDD) logging parameters.

Parameters

This command has one parameter:

logSetting	The desired logging behavior. Possible values are: *nolog* - Disables logging. *evtlog* - Logs all HDD events to the event log. *evtlogemail* - Logs all HDD events to the event log and enables email notification for these events, if email notification is enabled. *evtlogemailcallhome* - Logs all events to the event log and enables email notification and call home notification for these events, if email notification and call home notification are enabled.

Command example

```
Root> perf AFD HDDReport evtlog
```

perf.AFD.POMReport

Syntax

```
POMReport logSetting
```

Description

This command configures the Predictive Optics Monitoring (POM) event reporting configuration.

Parameters

This command has one parameter:

logSetting	The desired logging behavior. Possible values are: *nolog* - Disables logging. *evtlogemail* - Logs all POM events to the event log and enables email notification for these events, if email notification is enabled. *evtlogemailcallhome* - Logs all events to the event log and enables email notification and call home notification for these events, if email notification and call home notification are enabled.

Command example

```
Root> perf AFD POMReport evtlogemail
```

perf.AFD.show

Syntax

```
show
```

Description

This command displays all the configured settings under AFD.

Parameters

This command has no parameters.

Command example

```
Root> perf AFD show
```

Output

The configured settings are displayed as described in the following table:

HDD Logging	The current HDD logging value.
POM Logging	The current POM logging value.

Output example

```
Perf.AFD> show
HDD Report:    No logging
POM Report:    No logging
```

perf.class2

Syntax

```
class2 portNumber
```

Description

This command displays port Class 2 counters for a single port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 43000–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> perf class2 2
```

Output

The port Class 2 counter data is displayed as a table that includes the following statistics with a wrap count for each corresponding counter.

Port	The port number.
RxFrames	The number of Fibre Channel Class 2 frames that the port has received.
TxFrames	The number of Fibre Channel Class 2 frames that the port has transmitted.
RxWords	The number of Class 2 4-byte words within frames that the port has received.

TxWords	The number of Class 2 4-byte words within frames that the port has transmitted.
Busied Frms	The number of times the FBSY (Fabric Busy link response) was returned to this port as a result of a Class 2 frame that could not be delivered to the other end of the link. This occurs if either the fabric or the destination port is temporarily busy.
Rjct Frames	The number of times the FRJT (Frame Reject link response) was returned to this port as the result of a Class 2 frame that was rejected by the fabric.

Output example

The output from the *perf.class2* command displays as follows:

```
Port 2
Statistic            Wrap          Count
--------          -------------    ------------
RxFrames          23               2953184
TxFrames          12               1842953
RxWords           65               2953184
TxWords           32               1842953
Busied Frms       0                2953184
Rjct Frames       0                1842953
```

perf.class3

Syntax

```
class3 portNumber
```

Description

This command displays port Class 3 counters for a single port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 45000 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> perf class3 2
```

Output

The port Class 3 counter data is displayed as a table that includes the following statistics with a wrap count for each corresponding counter.

Port	The port number.
RxFrames	The number of Fibre Channel Class 3 frames that the port has received.
TxFrames	The number of Fibre Channel Class 3 frames that the port has transmitted.
RxWords	The number of Class 3 4-byte words within frames that the port has received.
TxWords	The number of Class 3 4-byte words within frames that the port has transmitted.
Disc Frames	The number of Class 3 frames that have been discarded upon receipt by this port. There are no FBSYs (Fabric Busy link response) or FRJTs (Frame Reject link response) generated for Class 3 frames.

Output example

The output from the *perf.class3* command displays as follows:

```
Port 2
Statistic               Wrap       Count
----------------        --------   --------
RxFrames                3          2953184
TxFrames                2          1842953
RxWords                 65         2953184
TxWords                 32         1842953
Disc Frames             26         2953184
```

perf.clearStats

Syntax

```
clearStats portNumber
```

Description

This command resets all port statistics for an individual port or for all ports.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 *all* for every port on the director or switch

Command example

```
Root> perf clearStats 4

Root> perf clearStats all
```

perf.errors

Syntax

```
errors portNumber
```

Description

This command displays port error counters for a single port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> perf errors 2
```

Output

The port error counter data is displayed as a table that includes the following statistics:

Port	The port number.
Prim Seq Err	The number of state machine protocol errors detected by the port hardware.
Disc Frms	The number of received frames discarded due to a frame size of less than size words or to frames dropped because the BB_Credit was zero. This number is counted during the first round of frame verification and applies to both Class 2 and Class 3 traffic.
Inv Tx Wrds	The number of 10-bit transmission words that the port is unable to map to 8-bit bytes because of disparity errors or misaligned K characters while in the OL2 or OL3 state.
CRC Errors	The number of frame CRC errors detected by the port.
Delim Errs	The number of invalid frame delimiters (SOF or EOF) received by the port.
Addr Id Errs	The number of frames received with unknown addressing.
FrmsTooShrt	The number of frames received that are too short.

Output example

The output from the *perf.errors* command displays as follows:

```
Port 2
StatisticCount
--------------------
Prim Seq Err753452
Disc Frms351269
Inv Tx Wrds2953184
CRC Errs1842953
Delim Errs2953184
Addr Id Errs1842953
FrmsTooShrt40059
```

perf.link

Syntax

```
link portNumber
```

Description

This command displays port link counters for a single port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> perf link 2
```

Output

The port link counter data is displayed as a table that includes the following statistics:

Port	The port number.
OLS In	The number of offline sequences initiated by the attached N_Port.
OLS Out	The number of offline sequences initiated by this switch or director port.
Reset In	The number of link resets initiated by the attached N_Port.
Reset Out	The number of link resets initiated by this switch or director.
LIPS In	The number of Loop Initialization Primitives (LIPs) detected on this switch loop port.
LIPS Out	The number of LIPs generated on this switch loop port.
Link FIrs	The number of times the port has detected a link error resulting from an invalid link state transition or timeout.
Sync Losses	The number of times the port has detected a loss of synchronization timeout while not in an offline or LF2 state.
Sig Losses	The number of times the port has detected a loss of signal while not in an offline or LF2 state.
Time at 0 Tx Credit	The number of 100 millisecond intervals where the switch port has zero Tx BB_Credit.

Output example

The output from the *perf.link* command displays as follows:

```
Port 2
Statistic               Count
-----------             ----------
OLS In                  753452
OLS Out                 351269
Reset In                2953184
Reset Out               1842953
Link Flrs               2953184
Sync Losses             1842953
Sig Losses              35246
Time at 0 Tx Credit     0
```

perf.openTrunking.backPressure

Syntax

```
backPressure backPressureState
```

Description

This command configures the Back Pressure state of the OpenTrunking configuration.

Parameters

This command has one parameter:

backPressureState	The enabled/disabled state of Open Trunking back pressure. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted. If the state is configured to be enabled, a back pressure entry is made to the Event Log and an SNMP trap is generated if SNMP is configured.

Command example

```
Root> perf openTrunking backPressure 1
```

perf.openTrunking.congestionThresh

Syntax

```
congestionThresh portNumber congestionThreshold
```

Description

This command configures the congestion threshold for an individual port or for all ports.

Parameters

This command has the following parameters:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 *all* applies the congestionThreshold value to every port on the product.
congestionThreshold	The congestion threshold in terms of percentage. Valid values are integers in the range 1 to 99 or *default*. Specifying the value *default* sets the specified port to the default threshold level of 10.

Command example

```
Root> perf openTrunking congestionThresh 8 20
```

perf.openTrunking.lowBBCreditThresh

Syntax

```
lowBBCreditThresh lowBBcreditThreshold
```

Description

This command configures the low BB_credit threshold of the OpenTrunking configuration. The low BB_credit threshold is defined as the percentage of time that no transmit BB_Credits are passed on the link. When the threshold value is exceeded, the system tries to reroute the flows that are going to the ISL with the problem. Effectively, the threshold is the percent of the time that the port does not receive BB_Credits before traffic is rerouted away from the port.

This threshold is also used for prevention of improperly rerouting to an ISL that lacks BB_Credits. In other words, the system does not reroute a flow to a link that lacks BB_Credits even if that link is significantly under its loading threshold. The system tries to reroute traffic away from a link that lacks BB_Credits, even if the loading threshold is significantly below the limit.

Parameters

This command has one parameter:

lowBBcreditThreshold	The low BB_credit threshold in terms of percentage. Valid values are integers in the range 1 to 99 or *default*. Specifying the value *default* sets the parameter to the default threshold level of 10%.

Command example

```
Root> perf openTrunking lowBBCreditThresh 20
```

perf.openTrunking.setState

Syntax

```
setState openTrunkingState
```

Description

This command enables or disables OpenTrunking feature. The OpenTrunking feature key must be installed to enable open trunking.

Parameters

This command has one parameter:

openTrunkingState	The enabled/disabled state of OpenTrunking feature. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> perf opentrunking setState 1
```

NOTE
The command "config.features.openTrunking" on page 29 has functionality that is identical to this command.

perf.openTrunking.show

Syntax

```
show portNumber
```

Description

This command displays the current OpenTrunking configuration per port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 4700 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> perf openTrunking show 11
```

Output

The OpenTrunking configuration data is displayed as a table that includes the following statistics:

Congestion Threshold	The threshold is listed as a percentage. If the value is a default value, `(default)` is displayed next to the percentage.
Flows Rerouted To	Trunking statistic displaying flows rerouted to the specified port. (These statistics are cleared by the *perf.clearStat*s command.)
Flows Rerouted From	Trunking statistic displaying flows rerouted from the specified port. (These statistics are cleared by the *perf.clearStat*s command.)
Unresolved Congestion	The current enabled/disabled state of the unresolved congestion trunking feature. (The indicated state applies to every port on the product.)
Backpressure	The current enabled/disabled state of the backpressure trunking feature. (The indicated state applies to every port on the product.)
Low BB_Credit Threshold	The current threshold setting of the Low BB_Credit Threshold trunking feature. If the value is a default value, `(default)` is displayed next to the percentage. (The indicated value applies to every port on the product.)

Output example

The output from the *perf.openTrunking.show* command displays as follows:

```
Port Number:                      1
Congestion Threshold (%):         56
Flows Rerouted To:                26739
Flows Rerouted From:              23987
Unresolved Congestion:            Enabled
Backpressure:                     Disabled
Low BB_Credit Threshold (%):      75 (default)
```

perf.openTrunking.unresCongestion

Syntax

```
unresCongestion unresolvedCongestionState
```

Description

This command configures the Unresolved Congestion state of the OpenTrunking configuration. If the state is configured to be enabled, an unresolved congestion entry is made to the Event Log and an SNMP trap is generated if SNMP is configured.

Parameters

This command has one parameter:

unresolvedCongestionState	The enabled/disabled state of the Unresolved Congestion state of the OpenTrunking configuration. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> perf openTrunking unresCongestion 1
```

perf.preferredPath

The *perf.preferredPath* commands enable you to use the preferred path feature to influence the route of data traffic that traverses multiple switches or directors in a fabric. If more than one ISL connects switches in your SAN, this feature is useful for specifying an ISL preference for a particular flow.

The preferred path feature allows you to enhance the path selection algorithm of the switch by providing the ability to prioritize ISLs for a selected port on the switch. The preferred path capability customizes the static load-balancing function by allowing you to specify an ISL preference for each remote domain. preferred path, however, is still subject to the standard Fabric Shortest Path First (FSPF) requirements, which allow the firmware to override the configuration setting if errors are encountered.

The data path consists of the source port of the switch or director being configured, the exit port of that switch or director, and the domain ID of the destination switch or director. Each switch or director must be configured for its part of the desired path in order to achieve optimal performance.

You may need to configure preferred paths for all switches or directors along the desired path for a proper multi-hop preferred path. (For examples of preferred path implementation and other related information, see the Element Manager manual your switch or product.)

The following rules apply when configuring preferred paths:

- The domain ID of the switch must be set to insistent.
- Domain IDs must be in the range of 1 -31.
- The specified numbers for source ports and exit ports must be in the range equal to the number of ports for the switch being configured.
- For any source port, only one path may be defined to each destination domain ID.

perf.preferredPath.clearPath

Syntax

```
clearPath destDomainID sourcePort
```

Description

This command deletes a preferred path. The command causes the specified path to use a path selection algorithm that is different from the preferred path. All configured paths can be removed by specifying the *all* parameter for both the destination domain ID and source port.

Parameters

This command has the following parameters:

destDomainId	The destination domain ID. Valid domain IDs are in the range 1–31 or *all*, which deletes all preferred paths to and from the source port specified in the sourcePort parameter.
sourcePort	The number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or you can specify *all* to delete all paths to the destination domain ID.

Command example

```
Root> perf preferredPath clearPath 10 5
```

perf.preferredPath.setPath

Syntax

```
setPath destDomainID sourcePort exitPort
```

Description

This command sets a preferred exit port, given the destination domain ID and source port. An exit port can be set for each combination of destination domain ID and source port.

NOTE
You cannot set a path where the Destination Domain ID is the same as the domain ID of the switch.

Parameters

This command has the following parameters:

destDomainId	The destination domain ID. Valid domain IDs are in the range 1–31.
sourcePort	The number of the source port. Valid port number values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 45000–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
exitPort	The number of the desired exit port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> perf preferredPath setPath 17 5 11
```

perf.preferredPath.setState

Syntax

```
setState enabledState
```

Description

This command enables or disables the preferred path feature.

NOTE
Insistent domain IDs must be used to enable the preferred path state.

Parameters

This command has one parameter:

enabledState	The enabled/disabled state of the preferred path feature. When disabled, the preferred path settings are ignored for all path selection decisions. Valid values are are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command example

```
Root> perf preferredPath setState enable
```

perf.preferredPath.showPath

Syntax

```
showPath destDomainID sourcePort
```

Description

This command displays the requested preferred path configuration. The output shows the configured preferred exit port. Using *all* for either the destination domain ID or the specified source port parameter results in an output that shows all configured and actual exit ports for the other parameter. If the destination domain is set to *all*, then all paths from the specified source port are displayed. If the source port is set to *all*, the output shows all source port paths to the specified domain. You cannot specify *all* for both the parameters.

Parameters

This command has the following parameters:

destDomainId	The destination domain ID. Valid domain IDs are in the range 1–31 or *all*, which shows all paths to and from the source port specified in the sourcePort parameter.
sourcePort	The number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or, you can specify *all* to show all paths to the destination domain ID specified for the destDomainId parameter.

Output

The output from the *perf.preferredPath.showPath* command includes the following parameters:

Destination Domain	The destination domain ID for which a preferred path has been configured. This is displayed only if the destination domain parameter is set to *all*.
Source Port	This is the source port for which a preferred path to the specified destination domain ID is specified. This is displayed only if the source port parameter is set to *all*.
Preferred Exit Port	The configured preferred path exit port. This value can be any port number, or blank to indicate that no preferred path has been configured.

Command and Output examples

The following examples show the output returned by the three methods of specifying the *perf.preferredPath.showPath* command.

Single values for both parameters

```
Root> perf preferredPath showPath 21 10
Preferred Path State: Enabled
Preferred Exit Port:  Not Configured
```

destDomainId set to all

```
Root> perf preferredPath showPath all 15
Preferred Path State: Enabled
Destination Domain  Preferred Exit Port
------------------  -------------------
1                   23
3                   24
4                   23
```

```
17                  12
```

sourcePort set to all

```
Root> perf preferredPath showPath 1 all
Preferred Path State: Enabled
Source Port         Preferred Exit Port
------------------  -------------------
0                   2
2                   5
3                   17
22                  5
```

perf.preferredPath.showState

Syntax

```
showState
```

Description

This command shows the enabled state for preferred path

Parameters

This command has no parameters.

Command example

```
Root> Perf PreferredPath showState
```

perf.slowdrainer.sdreport

Syntax

```
sdreport
```

Description

This command displays the report of slowdrainer

Parameters

This command has no parameters.

Command example

```
Root> Perf Slowdrainer SDReport
```

perf.slowdrainer.show

Syntax

```
show
```

Description

This command displays enabled state of slowdrainer

Parameters

This command has no parameters.

Command example

```
Root> Perf Slowdrainer show
```

Creating Threshold Alerts

The tasks you must complete to create and activate a threshold alert differ depending on the type of alert you are creating. To implement a counter threshold alert, see *Activating a Counter Threshold Alert* below. To implement a throughput alert, see "Activating a Throughput Threshold Alert" on page 189.

Activating a Counter Threshold Alert

To activate a counter threshold alert using the CLI, you must enter certain commands in the order specified in this section.

1. Create a counter threshold alert using the command "perf.thresholdAlerts.counter.addAlert" on page 191. Use this command to create a name for the threshold alert that you can use in subsequent commands. The threshold alert must then be configured using the other counter threshold alert commands.
2. Assign the threshold alert to a port using the command "perf.thresholdAlerts.counter.addPort" on page 192.
3. Configure the threshold alert using other *perf.thresholdalert* commands. For example, you may want to associate the threshold alert counter with the threshold alert name using the *perf.thresholdAlerts.counter.setCounter* command, described on page 194. Use the following commands to view alert settings and configure an alert:
   - "perf.thresholdAlerts.counter.removePort" on page 193
   - "perf.thresholdAlerts.counter.setCounter" on page 194
   - "perf.thresholdAlerts.counter.setParams" on page 195
   - "perf.thresholdAlerts.counter.show" on page 196
   - "perf.thresholdAlerts.counter.showStatisticTable" on page 196
4. Once the alert is fully configured, activate the alert using the *perf.thresholdAlerts.setState* command described on page 198. To modify an alert you need to disable it first.

Activating a Throughput Threshold Alert

To activate a throughput threshold alert using the CLI, you must enter certain commands in the specified sequence.

1. Create a throughput threshold alert using the command "perf.thresholdAlerts.throughput.addAlert" on page 200. Use this command to create a name for the threshold alert that you can use in subsequent commands. The threshold alert must then be configured using the other throughput threshold alert commands.
2. Assign the threshold alert to a port using the command "perf.thresholdAlerts.throughput.addPort" on page 201.
3. Identify the throughput statistic that triggers the throughput threshold alert using the command "perf.thresholdAlerts.throughput.setUtilType" on page 203.
4. Identify the percentage of throughput that triggers the throughput threshold alert using the command "perf.thresholdAlerts.throughput.setUtilPercentage" on page 204.
5. Configure the threshold alert using other perf.thresholdalert commands. For example, you may want to set the duration and interval times for the alert, as described in "perf.thresholdAlerts.throughput.setParams" on page 204. Use the following commands to view alert settings and configure an alert:
   - "perf.thresholdAlerts.throughput.removePort" on page 202
   - "perf.thresholdAlerts.throughput.setParams" on page 204
   - "perf.thresholdAlerts.throughput.show" on page 205
   - "perf.thresholdAlerts.throughput.showUtilTypeTable" on page 206
6. Once the alert is fully configured, it can be activated using the *perf.thresholdAlerts.setState* command, described on page 198. You need to disable an alert before you can modify it.

Alert Types and Counters

Table 5 provides a list of throughput threshold alerts.

TABLE 5 Throughput Threshold Alerts

Utilization Code	Threshold Alert Type
Tx Util	TTA - Transmit Utilization
Rx Util	TTA - Receive Utilization
Tx/Rx Util	TTA - Transmit or Receive Utilization

Table 6 provides a list of threshold alert counters and counter sets.

TABLE 6 Alert Counters

Number	Threshold Alert Counter or Counter Set
1	Link Resets Sent
2	Link Resets Received
3	OLS Sent
4	OLS Received

TABLE 6 Alert Counters (Continued)

Number	Threshold Alert Counter or Counter Set
5	Link Failures
6	Sync Losses
7	Signal Losses
8	Protocol Errors
9	Invalid Tx Word
10	CRC Errors
11	Discarded Frames
12	Discarded Frames
13	Delimiter Errors
14	Address ID Errors
15	Class2BusiedFrames
16	Class2RejectedFrames
17	Class3DiscardedFrames
18	Physical Link Errors Set
19	Link Sequence Counts Set
20	Logical Link Errors Set (see below)
21	LIPs Detected (Sphereon 4300 and Sphereon 4500 switches only)
22	LIPs Generated (Sphereon 4300 and Sphereon 4500 switches only)

Description of Summed Sets

Some of the threshold alerts consist of groups of related items called *Summed Sets*. When any of the items in the summed set are encountered, the total value of the summed set counter is incremented. The items that make up the summed sets are:

Physical Link Errors Summed Set

- Link Failures
- Sync Losses
- Signal Losses
- Protocol Errors
- Invalid Tx Words
- CRC Errors
- Frames Too Short
- Delimiter Errors

- Link Sequence Counts Summed Set
  - Link Resets Received

  - Link Reset Sent
  - OLS Received
  - OLS Sent

- Logical Link Errors Summed Set
  - Discarded Frames
  - Address ID Errors
  - Class 2 Busied Frames
  - Class 2 Rejected Frames
  - Class 3 Discarded Frames

perf.thresholdAlerts

The *perf.thresholdAlerts* commands enable you to configure alerts that notify you of specific conditions on your system.

You can configure a maximum of 16 threshold alerts, including both counter threshold alerts (CTAs) and throughput threshold alerts (TTAs). Each of these types of alerts have commands that are specific to the alert type.

- *Counter threshold alerts:* These are alerts that are triggered by counts of events. The commands used to configure these alerts start with *perf.thresholdAlerts.counter*.
- *Throughput threshold alerts:* These alerts are triggered by port throughput. The commands used to configure these alerts start with *perf.thresholdAlerts.throughput*.

For a list of the available threshold alert counters, see "Alert Types and Counters" on page 189.

perf.thresholdAlerts.counter.addAlert

Syntax

```
addAlert name
```

Description

This command configures a new counter threshold alert and assigns it a name. The new alert is assigned default settings which can then be changed using the other counter threshold alert commands.

The default settings for a new counter threshold alert are as follows:

- Ports: None
- Counter: None
- Increment: 100
- Interval: 60 minutes
- State: Disabled

Parameters

This command has one parameter:

name	The name of the new counter threshold alert. This name can consist of any ASCII characters up to a maximum length of 64 characters. To use spaces or special characters in this name, put quotation marks around the name. This parameter is case-sensitive.

NOTE
Although the system supports a name length of 64 characters, you may want to use a much shorter name. Some commands that display the threshold name show a maximum of 51 characters. If you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the commaDelim command. For more information, see "Using the commaDelim command" on page 15.

Command example

```
Root> perf thresholdAlerts counter addAlert checklinks
```

perf.thresholdAlerts.counter.addPort

Syntax

```
addPort name portNumber
```

Description

This command adds a port to the specified counter threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a counter threshold alert as defined by the command "perf.thresholdAlerts.counter.addAlert" on page 191.
portNumber	The port number or port type. Valid port number values: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 *all* applies the counter threshold alert to every port on the product.

Specifying a port type removes all the ports from the alert and applies the alert to each port that is the specified type of port. Valid values are:

- *eport*
- *fport*
- *flport* (Sphereon 4300 and Sphereon 4500 only)

NOTE
A counter threshold alert is not allowed to specify both port types and individual port numbers.

Command example

```
Root> perf thresholdAlerts counter addPort checklinks 12
```

perf.thresholdAlerts.counter.removePort

Syntax

```
removePort name portNumber
```

Description

This command removes a port from the specified counter threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a counter threshold alert as defined by the command *perf.thresholdAlerts.counter.addAlert*, described on page 191.
portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 *all* removes every port on the product from the counter threshold alert.

Command example

```
Root> perf thresholdAlerts counter removePort checklinks 12
```

perf.thresholdAlerts.counter.setCounter

Syntax

```
setCounter name counterNumber
```

Description

This command sets the counter statistic that is used to trigger the counter threshold alert. Use this command to associate a counter with the threshold alert name created using the *perf.thresholdAlerts.counter.addAlert* command.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a counter threshold alert as defined by the command *perf.thresholdAlerts.counter.addAlert*, described in page 191.
counterNumber	The counter number. Valid values are shown in Table 6.

Command example

```
Root> perf thresholdAlerts counter setCounter checklinks 1
```

perf.thresholdAlerts.counter.setParams

Syntax

```
setParams name increment interval
```

Description

This command sets the increment and interval times for a specified counter threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a counter threshold alert as defined by the command *perf.thresholdAlerts.counter.addAlert*, described on page 191.
increment	The number of times a counter must increment during the interval period to trigger the alert. Acceptable values are in the range of 1 to 70,560.
interval	The interval time in minutes for the alert. Acceptable values are in the range of 5 to 70,560 minutes.

Example

If ports 0,1, or 2 CRC Error counter increments more then 5 times within a period of 30 minutes, send an alert.

```
Port list = 0, 1, 2
CTA Counter = CRCErrors
Increment value= 5
Interval Time = 30
```

The increment value takes place in an interval that is a fixed length amount of time. This interval is not a rolling window interval.

Command example

```
Root> perf thresholdAlerts counter setParams checklinks 5 30
```

perf.thresholdAlerts.counter.show

Syntax

```
show name
```

Description

This command displays the settings for an individual counter threshold alert.

Parameters

This command has one parameter:

name	The name of a threshold alert as defined by the command *perf.thresholdAlerts.counter.addAlert*, described on page 191. You can specify *all* instead of a name, which means that all threshold alerts are displayed.

NOTE
The output of this command truncates threshold alert names that are longer than 51 characters. If you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the *commaDelim* command. For more information, see "Using the commaDelim command" on page 15.

Command example

```
Root> perf thresholdAlerts counter show checklinks
```

Output example

The output from the *perf.thresholdAlerts.counter.show* command displays as follows:

```
Index:              3
Name:               Example_CRC_Error_Finder
Ports:              2,4-7,20-24
Counter Statistic:  CRC Errors
Increment:          5
Interval:           30
Alert State:        Disabled
```

perf.thresholdAlerts.counter.showStatisticTable

Syntax

```
showStatisticTable
```

Description

This command displays the table of different statistic counters that can be added to a counter threshold alert. This table is used for reference only.

Parameters

This command has no parameters.

Command example

```
Root> perf threshAlerts counter showStatisticTable
```

Output example

The output from the *perf.thresholdAlerts.counter.showStatisticTable* command displays as follows:

```
Number   Counter or Counter Set
------   ----------------------
1         Link Resets Sent
2         Link Resets Rcvd
3         OLS Sent
4         OLS Received
5         Link Failures
6         Sync Losses
7         Signal Losses
8         Protocol Errors
9         Invalid Tx Words
10        CRC Errors
11        Discarded Frames
12        Frames Too Short
13        Delimiter Errors
14        Address ID Errors
15        Cls2 BusiedFrms
16        Cls2 RejectedFrms
17        Cls3 DiscardFrms
18        TimeWith0TxCredit
19        AverageTxBBCredit
20        AverageRxBBCredit
21        Phys Lnk Err Set
22        Lnk Seq Cnt Set
23        Logic Lnk Err Set
24        LIPs Detected
25        LIPs Generated
```

perf.thresholdAlerts.deleteAlert

Syntax

```
deleteAlert name
```

Description

This command deletes a specified threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has one parameter:

name	The name of a threshold alert as defined by the commands *perf.thresholdAlerts.counter.addAlert* and *perf.thresholdAlerts.throughput.addAlert*, or, enter *all* to delete all of the configured threshold alerts.

Command example

```
Root> perf thresholdAlerts deleteAlert checklinks
```

perf.thresholdAlerts.setState

Syntax

```
setState name enabledState
```

Description

This command enables or disables specified threshold alert.

Parameters

This command has the following parameters:

name	The name of a threshold alert as defined by the commands *perf.thresholdAlerts.counter.addAlert* and *perf.thresholdAlerts.throughput.addAlert*.
enabledState	The enabled/disabled state of the counter threshold alert. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> perf thresholdAlerts setState checklinks enabled
```

perf.thresholdAlerts.show

Syntax

```
show
```

Description

This command displays information about all threshold alerts.

Parameters

This command has no parameters.

Command example

```
Root> perf thresholdAlerts show
```

Output

The data is displayed as a table that includes the following properties:

Name	The name of the threshold alert (truncated to 51 characters).	
Type	The trigger statistic or threshold type of the alert (abbreviated to 17 chars).	
	Tx Util	TTA - Transmit Utilization
	Rx Util	TTA - Receive Utilization
	Tx/Rx Util	TTA - Transmit or Receive Utilization
	Link Resets Sent	CTA - Link Resets Sent
	Link Resets Received	CTA - Link Resets Received
	OLS Sent	CTA - OLS Sent
	OLS Received	CTA - OLS Received
	Link Failures	CTA - Link Failures
	Sync Losses	CTA - Sync Losses
	Signal Losses	CTA - Signal Losses
	Protocol Errors	CTA - Primitive Sequence Errors/Protocol Errors
	Invalid Tx Words	CTA - Invalid Tx Words
	CRC Errors	CTA - CRC Errors
	Discarded Frames	CTA - Discarded Frames
	Frames Too Short	CTA - Frames Too Short
	Delimiter Errors	CTA - Delimiter Errors
	Address ID Errors	CTA - Address ID Errors
	Cls2 BusiedFrms	CTA - Class 2 Busied Frames
	Cls2 RejectedFrms	CTA - Class 2 Rejected Frames
	Cls3 DiscardFrms	CTA - Class 3 Discarded Frames

	Phys Lnk Err Set	CTA - Physical Link Errors Summed Set
	Lnk Seq Cnt Set	CTA - Link Sequence Counts Summed Set
	Logic Lnk Err Set	CTA - Logical Link Errors Summed Set
	LIPs Detected	CTA - Loop Initialization Primitive Detected
	LIPs Generated	CTA - Loop Initialization Primitive Generated
State	The enabled state of the CTA. Either enabled or disabled.	

Output example

```
Name                                                Type               State
--------------------------------------------------  -----------------
--------
Throughput Threshold #1                              Rx Util            Enable
Threshold for CRC                                   CRC Errors         Disabled
Safety #2                                            Logic Lnk Err Set  Enabled
Safety #1                                           Cls2 BusiedFrms    Disabled
```

perf.thresholdAlerts.throughput.addAlert

Syntax

```
addAlert name
```

Description

This command configures a new throughput threshold alert and assigns it a name. The new alert is assigned default settings that can then be changed using the other throughput threshold alert commands.

The default settings for a new counter threshold alert are as follows:

- Ports: None
- Utilization Type: None
- Utilization Percentage: 50%
- Duration: 30 minutes
- Interval: 60 minutes
- Alert State: Disabled

Parameters

This command has one parameter:

name	The name of the new throughput threshold alert. This name can consist of any ASCII characters up to a maximum length of 64 characters. To use spaces or special characters in this name, put quotation marks around the name. This parameter is case-sensitive.

NOTE
Although the system supports a name length of 64 characters, you may want to use a much shorter name. Some commands that display the threshold name show a maximum of 51 characters. If you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the commaDelim command. For more information, see "Using the commaDelim command" on page 15.

Command example

```
Root> perf thresholdAlerts throughput addAlert port6Rx
```

perf.thresholdAlerts.throughput.addPort

Syntax

```
addPort name portNumber
```

Description

This command adds a port to the specified throughput threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a throughput threshold alert as defined by the command *perf.thresholdAlerts.throughput.addAlert*, described on page 200.
portNumber	The port number or port type. Valid values are either a single port number, all ports, or port type. The following port numbers are valid: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 4700 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 *all* applies the throughput threshold alert to every port on the product.

Specifying a *port type* removes the alert from all ports and applies the alert to all ports of the specified type. Valid values are:

- *eport*
- *fport*
- *flport* (Sphereon 4300 and Sphereon 4500 only)

NOTE
This parameter cannot specify both individual port numbers and a port type.

Command example

```
Root> perf thresholdAlerts throughput addPort eportRx eport
```

perf.thresholdAlerts.throughput.removePort

Syntax

```
removePort name portNumber
```

Description

This command removes a port from the specified throughput threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a throughput threshold alert as defined by the command *perf.thresholdAlerts.throughput.addAlert*, described on page 200.
portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 4700 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 *all* removes the throughput threshold alert from every port on the product.

Command example

```
Root> perf thresholdAlerts throughput removePort eportRx all
```

perf.thresholdAlerts.throughput.setUtilType

Syntax

```
setUtilType name utilizationType
```

Description

This command sets the throughput statistic that is used to trigger the throughput threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a throughput threshold alert as defined by the command *perf.thresholdAlerts.throughput.addAlert*, described on page 200.
utilizationType	The type of traffic that triggers the alert. Enter the number that corresponds to the desired utilization type: 1 - Transmit Traffic (Tx) 2 - Receive Traffic (Rx) 3 - Both (Rx and Tx)

Command example

```
Root> perf thresholdAlerts throughput setUtilType eportRx 1
```

perf.thresholdAlerts.throughput.setUtilPercentage

Syntax

```
setUtilPercentage name utilizationPercentage
```

Description

This command sets the throughput utilization percentage that is used to trigger the throughput threshold alert.

NOTE
An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters:

name	The name of a throughput threshold alert as defined by the command *perf.thresholdAlerts.throughput.addAlert*, described on page 200.
utilizationPercentage	The percentage of throughput utilization that triggers the alert. This must be entered as a number. Accepted values are in the range 1 to 100.

Command example

```
Root> perf thresholdAlerts throughput setUtilPercentage eportRx 70
```

perf.thresholdAlerts.throughput.setParams

Syntax

```
setParams name duration interval
```

Description

This command sets the name, duration, and interval for a specified throughput threshold alert. It also enables you to configure an alert to be sent when the following two events occur at the same time.

- The throughput threshold alert value is surpassed to more than the timespan specified in the duration parameter.
- The duration parameter is surpassed within the time frame specified by the interval parameter.

Parameters

This command has the following parameters:

name	The name of a throughput threshold alert as defined by the command *perf.thresholdAlerts.throughput.addAlert*, described on page 200.
duration	The duration time in minutes that the utilization must exist to trigger the alert. Acceptable values are in the range 0 to 70,560 minutes. Setting this value to zero means that the alert is triggered if the specified utilization is exceeded at any time. The value of this parameter must be less than or equal to the value of the interval parameter.
interval	The interval time in minutes. The interval is a fixed length of time. It is not a rolling window of time. Acceptable values are in the range 5 to 70,560 minutes. The value of this parameter must be greater than or equal to the value of the duration parameter.

Command example

```
Root> perf thresholdAlerts throughput SetParams eportRx 1 10
```

perf.thresholdAlerts.throughput.show

Syntax

```
show name
```

Description

This command displays the settings for an individual throughput threshold alert.

Parameters

This command has one parameter:

name	The name of a throughput threshold alert as defined by the command *perf.thresholdAlerts.throughput.addAlert*, described on page 200. You can also specify *all* instead of a name, to display all threshold alerts.

NOTE
The output of this command truncates all the threshold alert names that are longer than 51 characters. In case you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the commaDelim command. For more information, see "Using the commaDelim command" on page 15.

Command example

```
Root> perf thresholdAlerts throughput show eportRx
```

Output example

The output from the *perf.thresholdAlerts.throughput.show* command displays as follows:

```
Name:                    90% Receive Throughput Threshold
Ports:                   5,8,12,20-24
Utilization Type:        Rx
Utilization Percentage:  90%
Duration:                15
Interval:                30
Alert State:             Disabled
```

perf.thresholdAlerts.throughput.showUtilTypeTable

Syntax

```
showUtilTypeTable
```

Description

This command displays a table of the utilization types that can be used for a throughput threshold alert. This table is used for reference only.

Parameters

This command has no parameters.

Command example

```
Root> perf thresholdAlerts throughput showUtilTypeTable
```

Output example

The output from the *perf.thresholdAlerts.throughput.showUtilTypeTable* command displays as follows:

```
NumberUtilization Type
----------------------------
1   Transmit Traffic (Tx)
2   Receive Traffic (Rx)
3   Both (Tx/Rx)
```

perf.traffic

Syntax

```
traffic portNumber
```

Description

This command displays port traffic counters for a specified port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> perf traffic 2
```

Output

The port traffic counter data is displayed as a table that includes the following statistics, along with a wrap count for each corresponding counter.

Port	The port number.
Rx%	The received link utilization percentage.
Tx%	The transmitted link utilization percentage.
RxFrames	The number of Fibre Channel Class 2 and Class 3 frames that the port has received.
TxFrames	The number of Fibre Channel Class 2 and Class 3 frames that the port has transmitted.
RxWords	The number of 4-byte words in Class 2 and Class 3 frames that the port has received.
TxWords	The number of 4-byte words in Class 2 and Class 3 frames that the port has transmitted.

Output example

The output from the *perf.traffic* command displays as follows:

```
Port 2
Statistic            Wrap          Count
-----------          ----------    ----------
Rx%                  N/A           75
Tx%                  N/A           30
RxFrames             23            2953184
TxFrames             12            1842953
RxWords              65            2953184
TxWords              32            1842953
```

show

The *show* branch of the CLI command tree contains commands that display, but do not change, stored data values. The displayed output that results from these commands is not necessarily identical with the output from the show commands that are within the other CLI command tree branches, for example, *config.port.show*.

The commands in the show branch can by used by either the administrator or the operator.

show.activeAlias

Synopsis

```
activeAlias
```

Description

This command displays the active WWN aliases.

Parameters

This command has no parameters.

Command example

```
Root> show activeAlias
```

Output

The following attributes are displayed by this command.

CLI Alias enabled state	The CLI enabled/disabled state of WWN aliases.
WEB Alias enabled state	The WEB enabled/disabled state of WWN aliases.
Total associations possible	The total number of possible associations.
Current association count	The number of configured associations.
WWN	The WWNs with configured aliases.
Alias	The Aliases associated with the WWNs.

Output example

```
show> activeAlias
CLI Alias enabled state:        Disabled
Web Alias enabled state:        Disabled
Total Associations Possible:    250
Current Association Count:      9
WWN                     Alias
----------------------  ------------------------
11:22:33:44:55:66:77:01  NAME1
11:22:33:44:55:66:77:02  NAME2
11:22:33:44:55:66:77:03  NAME3
11:22:33:44:55:66:77:04  NAME4
```

show.all

Syntax

```
all
```

Description

This command displays all configuration and status information that is available. The command results in a sequential display of the output of other CLI *show* commands. This set of show commands returns the full configuration and status of the switch and fabric.

Parameters

This command has no parameters.

Command example

```
Root> show all
```

Output

The output of this command is a sequential display of the output of other CLI *show* commands. The commands are displayed in the following order:

- *show.ip.ethernet*
- *show.system*
- *show.switch*
- show.openSysMS.config
- *show.port.config*
- *show.frus*
- *config.snmp.show*
- *show.zoning*
- *show.port.state*
- *show.port.info*
- *show.port.technology*
- *show.loginserver*
- *show.features*
- *show.security.portbinding*
- *show.security.switchbinding*
- *show.security.fabricbinding*
- *show.openTrunking.config*
- *show.thresholdAlerts.alerts*
- *show.fabric.topology*
- *show.fabric.nodes*
- *show.security.switchACL*
- *show.ficonCUPZoning*
- *show.fencing.Policies*
- *show.activeAlias*

show.auditLog

Syntax

```
auditLog [clear]
```

Description

This command displays the entries of the audit log after the last time the log was cleared.

Parameters

This command has one optional parameter:

clear	Whether all entries should be cleared from the log. If the log is full, it resumes collecting log entries.

Command example

```
show auditLog
```

Output

The output from this command displays the following data:

Date/Time	The date and time of the log entry.
Action	Type of audit log event.
Source	Source of audit log event.
User ID	Identifier of the user that made the command. Usually an IP address.

Output example

```
Date/Time         Action            Source     User Id
----------        -----------       -------    -------------
11/24/03 04:18P   Switch set online     CLI     172.16.22.23
11/24/03 03:38P   Switch name modified CLI     172.16.22.23
11/24/03 03:38P   Switch set offline   CLI     172.16.22.23
11/24/03 11:27A   Firmware downloaded  Web     172.60.5.40
```

show.epFrameLog.config

Syntax

```
config
```

Description

This command shows the current embedded port frame log settings.

Parameters

This command has no parameters.

Command example

```
Root> show epFrameLog config
```

Output

The output from this command contains the following data:

Filter Class F Frames	If enabled, filtering of Class F frames takes place.
Filter Port	The port that is being filtered on.
Trigger State	The state of the trigger. Active if the trigger conditions have not been met.
Num of Entries	Number of frames that have been logged since the start condition was met.
Start offset	The number of bytes into the frame to where the start bit pattern is looked for.
Start Bit Pattern	The bit pattern that triggers the logging to begin.
End Offset	The number of bytes into the frame to where the end bit pattern is looked for.
End Bit Pattern	The bit pattern that triggers the logging to end.
Start Condition Met	True if the start condition was met.
End Condition Met	False if the end condition was not met.

Command example

```
Root> show EPFrameLog config

Filter Class F Frames:   Disabled
Filter Port:             15
Start Offset:            0
Start Bit Pattern:       FFXXXXX3452
End Offset:              0
End Bit Pattern:         FBXXXXX3321
Trigger State:           Active
Num of Entries:          6
Start Condition Met:     True
End Condition Met:       False
```

show.epFrameLog.disableTrigger

Syntax

```
disableTrigger
```

Description

This command clears the embedded port frame log trigger, which was configured with the command *show.epFrameLog.setTrigger*.

Parameters

This command has no parameters.

Command example

```
Root> show epFrameLog disableTrigger
```

show.epFrameLog.filterClassFFrames

Syntax

```
filterClassFFrames [enable]
```

Description

This command turns on or turns off the ability to filter out Class-F frames, or shows the current state of this filtering.. When the filtering is enabled, everything but Class-F frames are logged. This setting is not stored in NVRAM and does not persist after IML.

Parameters

This command has one optional parameter. If no parameters are entered, it displays the current state.

filterstate	The on/off state. Valid values are *enable* and *disable*. Boolean 1 and 0 values may also be substituted.

Command example

```
Root> show epFrameLog filterClassFFrames enable
```

show.epFrameLog.noWrap

Syntax

```
noWrap [clear]
```

Description

This command displays the contents of the non-wrapping region of the FC2 frame log. Specifying the optional keyword clear removes all entries from the non-wrapping region of the log.

The log entries do not persist over IMLs or power cycles; it is not stored in NVRAM. This log does not include entries for frames discarded by hardware such as un-routable Class-3 frames, unless Class-3 discard is disabled in the hardware.

NOTE
This log will not wrap. The log stops collecting entries after is it filled.

Parameters

This command has one optional parameter. If no parameter is specified, then the 500 entries of the log are displayed.

clear	Whether all entries should be removed from the non-wrapping region of the log.

Command example

```
Root> show epFrameLog noWrap
```

Output

This command displays the following data:

Count	A constantly incrementing counter.
Date/Time	Time of the frame.
Port #	The port number.
Direction	Direction of the frame through the port (I = In, O = Out, D= Discard).
SOF	Start of frame.
EOF	End of frame.
Header	The 24 byte FC frame header.
PL (size in bytes)	The first 32 bytes of the FC frame payload.

Output example

The output of the show.epFrameLog.nowrap command displays as follows:

```
Count  Date/Time         Port #     Direction  SOF     EOF            Payload
Size
------ ---------------   ------     ---------  ---     --- ------------
39     11/24/03 11:30A   39         O          i3      n      2112
Header: 22000026 000000EF E1000000 00000000 FFFF0000 00000000
PL:     00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
1C1D1E1F
38     11/24/03 11:30A   38         I          i3      n      2112
Header: 22000026 000000EF E1000000 00000000 FFFF0000 00000000
PL:     00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
1C1D1E1F
```

```
37     11/24/03 11:30A   38         O          i3     n      2112
Header: 22000025 000000EF E1000000 00000000 FFFF0000 00000000
PL:     00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
1C1D1E1F
```

show.epFrameLog.removeFilterPort

Synopsis

```
removeFilterPort portNumber
```

Description

This command removes a port from the FC2 frame logging filter.

Parameters

This command has one parameter:

portnumber	The port number to be removed from FC2 filtering, or all to disable FC2 frame log for all the ports. Valid Port Numbers range from: 0–11 for the Sphereon 4300 0–16 for the Sphereon 3016 and Sphereon 4400 0–24 for the Sphereon 4500 0–32 for the Sphereon 3032 and Sphereon 4700 0–64 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> show epFrameLog removeFilterPort 10
```

show.epFrameLog.setFilterPort

Syntax

```
setFilterPort portNumber
```

Description

This command adds a port number to a list of ports that are filtered for FC2 frame log. This setting is not be stored in NVRAM and does not persist after IML.

Parameters

This command has one parameter.

Port Num	The port number to specify “all” for disabling FC2 frame log for all the ports or the port number for which frame log entries are recorded. Valid Port Numbers range from: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 [all] The “all” parameter makes the FC2 log collect entries from all of the ports on the switch. [none] The “none” parameter makes the FC2 log stop collecting entries.

Command example

```
Root> show epFrameLog setFilterPort 63
```

show.epFrameLog.setTrigger

Syntax

```
setTrigger portNumber offStart bitStart offEnd bitEnd
```

Description

This command sets a logging trigger value for the embedded port frame log.

Parameters

This command has five parameters:

portNumber	The port to monitor this trigger on. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
offStart	The offset for the start bit pattern.

bitStart	The bit pattern that triggers the logging. 'X' or 'x' can be used as a wild card.
offEnd	The offset for the end bit pattern.
bitEnd	The bit pattern that ends the logging. 'X' or 'x' can be used as a wild card.

Command example

```
show.EPFrameLog> setTrigger 5 0 FFXXXXX3452 0 FBXXXXX3321
```

NOTE
Once the trigger conditions have been met, you must clear the filter manually. No new entries are written to the frame log until you initiate it.

show.epFrameLog.wrap

Syntax

```
wrap [clear]
```

Description

This command displays the contents of the wrapping region of the FC2 frame log. Specifying the optional keyword *clear* clears all entries from both the wrapping and the non-wrapping regions of the log.

The log entries do not persist over IMLs or power cycles, and are not stored in NVRAM. This log does not includes entries for frames discarded by hardware, such as un-routable class-3 frames unless class-3 discard is disabled in the hardware.

NOTE
This log begins to wrap after the log is filled.

Parameters

This command has one optional parameter. If no parameter is specified, then the 1000 entries of the log are displayed.

clear	Whether all entries from both the wrapping and the non-wrapping regions of the log should be removed.

Command example

```
Root> show epFrameLog wrap
```

Output

This command displays the following data:

Count	A constantly incrementing counter.
Date/Time	Time of the frame.
Port #	The port number.
Direction	Direction of the frame through the port (I = In, O = Out, D= Discard).
SOF	Start of frame.
EOF	End of frame.
Header	The 24 byte FC frame header.
PL (size in bytes)	The first 32 bytes of the FC frame payload.

Output example

The output of the show.epFrameLog.wrap command displays as follows:

```
Count      Date/Time         Port #     Direction  SOF    EOF
Payload Size
------     ---------------   ------     ---------  ---    --- -------------
39         11/24/03 11:30A   39         O          i3     n      2112
Header: 22000026 000000EF E1000000 00000000 FFFF0000 00000000
PL:     00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
38         11/24/03 11:30A   38         I          i3     n      2112
Header: 22000026 000000EF E1000000 00000000 FFFF0000 00000000
PL:     00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
37         11/24/03 11:30A   38         O          i3     n      2112
Header: 22000025 000000EF E1000000 00000000 FFFF0000 00000000
PL:     00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

show.eventLog

Syntax

```
eventLog [clear]
```

Description

This command displays the contents of the event log as maintained in NV-RAM on the director or switch.

Parameters

This command has one parameter:

clear	Whether all event log entries should be cleared.

Command example

```
Root> show eventLog
```

Output

The event log data are displayed as a table that includes the following properties.

Date/Time	The date and time when the event occurred.
Code	The event reason code.
Severity	The severity of the event. The values are: **Major**—Unit operational (major failure). **Minor**—Unit operational (minor failure). **Severe**—Unit not operational. The causes are either that the switch contains no operational SBAR cards or that the system shuts down due to CTP thermal threshold violations. **Info**—Unit operational (information only).
FRU	The FRU and FRU position, where applicable.
Event Data	The 32-byte hexadecimal description of the event in words.

Output example

The output from the *show.eventLog* command displays as follows:

```
Date/Time         Code  Severity  FRU    Event Data
----------------  ----  --------  -----  ----------------------------------
04/12/01  10:58A  375   Major     CTP-0  00010203 04050607 08090A0B 0C0D0E0F
04/12/01   9:58A  385   Severe    CTP-0  00010203 04050607 08090A0B 0C0D0E0F
04/11/01   7:18P  395 Severe    CTP-0  00010203 04050607 08090A0B 0C0D0E0F
```

show.fabric.agshow

Syntax

```
Show.fabric.agshow
```

Description

This command displays a list of all fabric attached agdevices (both local and remote). It is supported only in 6140, 4400 and 4700.

Parameters

This command has no parameters.

Output

```
Root> show fabric agshow
```

```
     worldwide name      Ports  Enet IP address  Firmware LocalRemote   Name
---------------------  -----  ---------------  --------  ---------  -----------
10:00:00:05:1E:5F:50:52 16     172.26.22.203    v6.2.00   1          swd77
worldwide name      Ports  Enet IP address  Firmware LocalRemote   Name
---------------------  -----  ---------------  --------  ---------  -----------
10:00:00:05:1E:0A:16:59 16     172.26.22.205    v6.2.0    0          swd77
```

show.fabric.agshow local

Syntax

```
Show.fabric.agshow local
```

Description

This command displays only the locally attached agdevices. It is supported only in 6140, 4400 and 4700.

Parameters

This command has no parameter

Output

```
Show.Fabric> agshow local
     worldwide name      Ports  Enet IP address  Firmware LocalRemote   Name
---------------------  -----  ---------------  --------  ---------  -----------
10:00:00:05:1E:5F:50:52 16     172.26.22.203    v6.2.00   1          swd77
Show.Fabric>
```

show.fabric.agshow remote

Syntax

```
show.fabric.agshow Remote
```

Description

This command displays only a list of remote agdevices . It is supported only in 6140, 4400 and 4700.

Parameters

This command has no parameter

Output

```
agshow remote
This command could take up to 12 seconds
     worldwide name      Ports  Enet IP address  Firmware LocalRemote   Name
```

```
---------------------  -----  ---------------  --------  ---------  -----------
10:00:00:05:1E:0A:16:59 16     172.26.22.205    v6.2.0    0          swd77
Show.Fabric>
```

show.fabric.dcfmtable

Syntax

```
show.fabric.Dcfmtable
```

Description

This command displays the fabric information (seed switch) of all the switches in the fabric. It is supported only in 6140, 4400 and 4700.

M-EOSc swtiches are independant of vfid, so the vfid information is displayed as -1.

The model number and the subsequent switch type is given in the table below.

Model No	Switch Type
224	Intrepid 10000
225	Intrepid 6140
226	Intrepid 6064
227	ED 5000 Director
228	Sphereon 4500
229	Sphereon 4300
230	Sphereon 4700
231	Sphereon 4400
232	Rainier 32 w/ 10G (4710)
233	Sphereon 3032
234	Sphereon 3232
235	Sphereon 3016
236	Sphereon 3216

Parameters

This command has no parameter.

Output

```
Root> show fabric dcfmtable
Domain ID:           5
WWN:                 10:00:08:00:88:04:9C:BB
IP address:          172.26.22.237
IPv6 address:        ::
Firmware version:    Release 09.09.01, Build 9
Vendor name:         McDATA Corporation
model:               234
VF_ID:               -1

Domain ID:           8
WWN:                 10:00:08:00:88:04:9C:3C
```

```
IP address:          172.26.22.245
IPv6 address:        2202:1:2:3:4:5:8:7
Firmware version:    Release 09.09.01, Build 9
Vendor name:         McDATA Corporation
model:               225
VF_ID:               -1

Domain ID:           10
WWN:                 10:00:08:00:88:45:AE:00
IP address:          172.26.22.51
IPv6 address:        ::
Firmware version:    Release 9.9.2, Build 7
Vendor name:         McDATA Corp.
model:               224
VF_ID:               -1
```

show.fabricLog.noWrap

Syntax

```
noWrap [clear]
```

Description

This command displays the contents of the non-wrapping region of the fabric log. The log entries do not persist over IMLs or power cycles; it is not be stored in NVRAM.

NOTE
This log will not wrap. The log stops collecting entries after is it filled.

Parameters

This command has one optional parameter. If no parameter is specified, then the 200 entries of the log are displayed.

clear	Whether all entries should be removed from the log.

Command example

```
Root> show fabricLog noWrap
```

Output

This command displays the following data:

Count	A constantly incrementing counter.
Date/Time	The date and time of the log entry.
Description	A description of the log entry.
Data	Extended data that is associated to the log entry.

Output example

The output of the *show.fabricLog.noWrap* command displays as follows:

```
Count          Date/Time            Description
----------     ---------------      -------------
11             11/24/03 04:18P      Port RSCN
Data: RSCN Reason=2301, Port Offline/Online=26437, Ports 0, 1, 2, 3, 4, 5, 6,
    7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,
    25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 40, 41, 42,
    43, 44, 45, 46, 47, 48, 49,50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60,
    61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78,
    79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96,
    97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111,
    112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125,
    126, 127, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143,
144
10             12/04/03 08:15A      Fabric Operational
Data:
9              12/04/03 08:15A      Paths Operational
Data:
8              12/04/03 08:15A      Zone Merge Completed
```

show.fabricLog.wrap

Syntax

```
wrap [clear]
```

Description

This command displays the contents of the wrapping region of the fabric log. The log entries do not persist over IMLs or power cycles; it is not stored in NVRAM.

NOTE
This log begins to wrap after the log is filled.

Parameters

This command has one optional parameter. If no parameter is specified, then the 1000 entries of the log are displayed.

clear	Whether all entries should be removed from the log.

Command example

```
show fabricLog Wrap
```

Output

This command displays the following data:

Count	A constantly incrementing counter.
Date/Time	The date and time of the log entry.
Description	A description of the log entry.
Data	Extended data that is associated to the log entry.

Output example

The output of the *show.fabricLog.wrap* command displays as follows:

```
Count          Date/Time            Description
----------     ---------------      -------------
11             11/24/03 04:18P      Port RSCN
Data: RSCN Reason=2301, Port Offline/Online=26437, Ports 0, 1, 2, 3, 4, 5, 6,
    7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,
    25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 40, 41, 42,
    43, 44, 45, 46, 47, 48, 49,50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60,
    61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78,
    79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96,
    97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111,
    112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125,
    126, 127, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143,
144
10             12/04/03 08:15A      Fabric Operational
Data:
9              12/04/03 08:15A      Paths Operational
Data:
8              12/04/03 08:15A      Zone Merge Completed
Data:
```

show.fabric.nodes

Syntax

```
nodes
```

Description

This command displays a list of all fabric-attached nodes.

Parameters

This command has no parameters.

Command example

```
Root> show fabric nodes
```

Output

The data is displayed as a table that includes the following properties:

Domain ID	Domain ID of the switch to which the device is attached.
Node WWN	The Node WWN of the fabric attached node.
Port WWN	The Port WWN of the fabric attached port.

Output example

The output from the s*how.fabric.node*s command displays as follows:

```
Domain ID  Node WWN                  Port WWN
---------  ------------------------  ------------------------
3          6C:61:62:01:3A:C5:CC:BF   6C:61:62:01:3A:C6:0D:87
```

show.fabric.ping

Syntax

```
ping destination [count] [timeout]
```

Description

This command issues a ping request to the specified destination.

Parameters

This command has three parameters.

destination	The destination of ping request. This parameter can be an FC ID or the WWN of the destination in the fabric.
count	Optional. The number of times the destination is to be sent the ping request. Default is 4. Maximum count possible is 10.
timeout	Optional. The time the command waits before timing out. Default is 5. Maximum possible timeout is 10.

Command example

```
Root> show fabric ping 6F0613
```

Output

Time taken (ms)	The time taken to get reply from the destination.

Output example

```
Ping 6F0613
Show.Fabric> ping 6F0613
This command may take up to 20s to complete
Received response from 6F0613 in 57ms.
Received response from 6F0613 in 57ms.
Received response from 6F0613 in 52ms.
Received response from 6F0613 in 58ms.

Show.Fabric> ping 6F0713
This command may take up to 20s to complete
Received response from 6F0713 in 400ms.
Response from 6F0713 timed out
Received response from 6F0713 in 95ms.
Received response from 6F0713 in 80ms.
```

show.fabric.principal

Syntax

```
principal
```

Description

This command displays the WWN of the principal switch in the fabric.

Parameters

This command has no parameters.

Command example

```
Root> show fabric principal
```

Output

The data is displayed as a table that includes the following properties:

Principal Switch WWN	The WWN of the principal switch in the fabric.

Output example

```
Principal Switch WWN:       00:00:00:00:00:00:00:00
```

show.fabric.showRouteTable

Syntax

```
showRouteTable [source] [destination]
```

Description

This command displays routes for specified online ingress port to specified domains in the fabric.

Parameters

This command has two parameters, which are optional.

source	The source port/Ingress port for which the route table is displayed.
destination	The destination Domain ID for which the route is displayed.

NOTE
If a parameter is not mentioned, then all the online ports and domains are displayed.

Command example

```
Root> show fabric showRouteTable
```

Output

The data is displayed as a table that includes the following properties:

Ingress	The ingress port on the switch.
DID	The destination Domain ID.
Egress	The egress port on the switch.
Rem DID	The neighboring switch's Domain ID.
Rem Ingress	The ingress port on the neighboring switch.
Hops	The number of hops the route makes to reach the neighboring DID.
Act Cost*	True cost of the link based on the port speed.
Eff Cost*	This is the FSPF cost of routing.
Path	Whether the path is a Preferred Path. Valid values are *Yes* or *No*.

* The actual cost and effective cost can be different based on whether ISL cost configuration is configured or not. If ISL cost configuration is configured, then links with different speeds will have different costs (1G = 1000, 2G = 1000, 4G = 250, 10G = 100). Actual cost lists the actual cost that based on the cost configuration and effective cost is the cost assuming that the ISL cost configuration is not configured.

Output example

```
Show.Fabric> showRouteTable
Ingress  DID  Egress  Rem Did  Rem Ingress  Hops  Act Cost  Eff Cost  PPath
-------  ---  ------  -------  -----------  ----  --------  --------  -----
1        3    2       3        3            1     1000      1000      No
1        9    5       9        3            1     1000      1000      No
2        1    1       6        63           3     3000      3000      No
2        6    1       6        63           1     1000      1000      No
2        9    5       9        3            1     1000      1000      No
2        10   1       6        63           2     2000      2000      No
5        1    1       6        63           3     3000      3000      No
5        3    2       3        3            1     1000      1000      No
5        6    1       6        63           1     1000      1000      No
5        10   1       6        63           2     2000      2000      No


Show.Fabric> showRouteTable 5
Ingress  DID  Egress  Rem Did  Rem Ingress  Hops  Act Cost  Eff Cost  PPath
-------  ---  ------  -------  -----------  ----  --------  --------  -----
5        1    1       6        63           3     3000      3000      No
5        3    2       3        3            1     1000      1000      No
5        6    1       6        63           1     1000      1000      No
5        10   1       6        63           2     2000      2000      No

Show.Fabric> showRouteTable 5 10
Ingress  DID  Egress  Rem Did  Rem Ingress  Hops  Act Cost  Eff Cost  PPath
-------  ---  ------  -------  -----------  ----  --------  --------  -----
5        10   1       6        63           2     2000      2000      No
```

show.fabric.topology

Syntax

```
topology
```

Description

This command displays a text description of the fabric. The principal switch in the fabric will have an asterisk (*****) next to it.

Parameters

This command has no parameters.

Command example

```
Root> show fabric topology
```

Output

The features data is displayed as a table that includes the following properties.

Switch WWN	The WWN of the switch at the local end of the ISL.
DID	The Domain ID of the switch at the local end of the ISL.
OutPrt	The port number at the local end of the ISL.
Remote WWN	The WWN of the switch at the remote end of the ISL.
RemDID	The domain ID of the switch at the remote end of the ISL.
RemPrt	The port number at the remote end of the ISL.

Output example

The output from the *show.fabric.topology* command displays as follows:

```
Switch WWN               DID  OutPrt  Remote WWN               RemDID  RemPrt
-----------------------  ---  ------  -----------------------  ------  ------
02:30:40:32:34:34:32:21* 2    24      24:45:73:49:05:43:22:11  10      2
                              25      24:45:73:49:05:43:22:11  10      3
                              26      24:45:73:49:05:43:22:11  10      4
24:45:73:49:05:43:22:11  10   2       02:30:40:32:34:34:32:21  2       24
                              3       02:30:40:32:34:34:32:21  2       25
                              4       02:30:40:32:34:34:32:21  2       26
21:23:21:25:76:43:23:21  10   7       02:30:40:32:34:34:32:21  15      3
02:30:40:32:34:34:32:21  15   3       21:23:21:25:76:43:23:21  10      7
```

show.fabric.traceRoute

Syntax

```
traceRoute source destination
```

Description

This command retrieves the route between two nodes in the fabric.

Parameters

This command has two parameters:

source	The source port for the trace route. This can be either a Port ID or a WWN.
destination	The destination port for the trace route. This can be either a Port ID or a WWN.

Command example

```
Root> show fabric traceRoute
```

Output

Return code	The return value. Possible values are: Command Completed Successfully Command Not Supported in Next Switch No Response from Next Switch Maximum Hop Count Reached Source Port not in Fabric Destination Port not in Fabric Devices not in Common Zone No Route Between Designated Ports No Additional Explanation Fabric Busy Fabric Build in Progress Unable to run a trace route at this time
Number of Entries	The number of entries returned from the trace route.
Switch WWN	The switch WWN at that point in the trace route.
Domain ID	The switch Domain ID at that point in the trace route.
Ingress Port WWN	The Ingress Port WWN taken by the trace route.
Ingress Port Num	The Ingress Port Num taken by the trace route.
Egress Port WWN	The Egress Port WWN taken by the trace route.
Egress Port Num	The Egress Port Num taken by the trace route.
Direction	The direction the trace route was going for the specified entry. Possible values are: Source to destination At Destination Destination to source

Output example

Show.Fabric> traceroute 50:06:04:8D:C7:DF:AE:A0 50:06:04:8D:C7:DF:AE:9F

```
Return code:          Command Completed Successfully
Number of Entries:    6

Entry 0
Switch WWN:           10:00:08:00:88:60:F0:A2
Domain ID:            26
Ingress Port WWN:     20:15:08:00:88:60:F0:A2
Ingress Port Num:     17
Egress Port WWN:      20:0D:08:00:88:60:F0:A2
Egress Port Num:      9
Direction:            Source to destination
```

```
Entry 1
Switch WWN:           10:00:08:00:88:22:33:44
Domain ID:            2
Ingress Port WWN:     20:17:08:00:88:22:33:44
Ingress Port Num:     19
Egress Port WWN:      20:1B:08:00:88:22:33:44
Egress Port Num:      23
Direction:            Source to destination

Entry 2
Switch WWN:           10:00:08:00:88:A0:B0:9C
Domain ID:            31
Ingress Port WWN:     20:12:08:00:88:A0:B0:9C
Ingress Port Num:     14
Egress Port WWN:      20:0F:08:00:88:A0:B0:9C
Egress Port Num:      11
Direction:            At destination

Entry 3
Switch WWN:           10:00:08:00:88:A0:B0:9C
Domain ID:            31
Ingress Port WWN:     20:0F:08:00:88:A0:B0:9C
Ingress Port Num:     11
Egress Port WWN:      20:12:08:00:88:A0:B0:9C
Egress Port Num:      14
Direction:            Destination to source

Entry 4
Switch WWN:           10:00:08:00:88:22:33:44
Domain ID:            2
Ingress Port WWN:     20:1B:08:00:88:22:33:44
Ingress Port Num:     23
Egress Port WWN:      20:17:08:00:88:22:33:44
Egress Port Num:      19
Direction:            Destination to source

Entry 5
Switch WWN:           10:00:08:00:88:60:F0:A2
Domain ID:            26
Ingress Port WWN:     20:0D:08:00:88:60:F0:A2
Ingress Port Num:     9
Egress Port WWN:      20:15:08:00:88:60:F0:A2
Egress Port Num:      17
Direction:            Destination to source
```

show.features

Syntax

```
features
```

Description

This command displays a table of all installed feature sets and their states. This command provides the same output as the command "config.features.show" on page 30.

Parameters

This command has no parameters.

Command example

```
Root> show features
```

Output

The features data is displayed as a table that includes the following properties:

Installed Feature Set	The feature set installed using a feature key. Only installed keys are displayed.
Feature	Individual features within each set. In many cases, there is only one feature within each feature set.
State	The state of the individual feature. Fabric-wide features are displayed as Active/Inactive. Switch-centric features are displayed as Enabled/Disabled.
Exp	The remaining evaluation time in days for the trial feature.

Output example

The output from the *show.feature*s command displays as follows:

```
Installed Feature Set           Feature                         State     Exp
------------------------------  ------------------------------  --------  -----
Security Package
  SANtegrity Binding            Switch Binding                  Enabled
  SANtegrity Binding            Fabric Binding                  Active
  SANtegrity Binding            Enterprise Fabrics              Active
  SANtegrity Authentication     SANtegrity Authentication       Enabled

FICON Cascading Bundle
  FICON Management Server       FICON Management Server         Enabled
  FICON CUP Zoning              FICON CUP Zoning                Active
  OpenTrunking                  OpenTrunking                    Active
```

NOTE
If a feature is present in two bundles, it is displayed in only one bundle under *Installed Feature Set* property.

show.fencing.policies

Syntax

```
fencing [name]
```

Description

This command displays a table of the configured fencing policies. If a specific policy name is given, then a full description of the policy is shown.

Parameters

This command has one optional parameter, an individual policy name. If an individual policy name is given, then a detailed description is displayed for the specified policy. If no parameter is given, then a summary of all policies is displayed.

Command example

```
Root> show fencing
Root> show fencing Protocol Errors #2
```

Output

The data is displayed as a table that includes the following properties:

Name	The name of the policy. This is concatenated to 50 characters in the summary display. The policy full name is displayed in comma-delim mode.
Ports	The ports to which the fencing policy is applied.
Type	The type of the fencing policy.
Limit	The number of offenses that are allowed before a port is disabled.
Period	The amount of time that limit of number of offenses must exceed before a port is fenced.
State	The enabled state of the fencing policy.

Output example

```
Root> show fencing
Name                        Type              State
-------------------------   ---------------   --------
Default_Protocol_Errors     Protocol Errors   Enabled
Protocol Errors #2          Protocol Errors   Disabled
Safety #2                   Protocol Errors   Enabled

Root> show fencing Protocol Errors #2
Name:          Protocol Errors #2
Ports:         2,4-7,20-24
Type:          Protocol Errors
Limit:         5
Period:        1800 seconds
State:         Disabled
```

show.ficonCUPZoning

Syntax

```
ficonCUPZoning
```

Description

This command displays the contents of the host control list and the enabled state of FICON CUP Zoning.

NOTE
The command "config.ficonCUPZoning.show" on page 39 has functionality that is the same as this command.

Parameters

This command has no parameters.

Command example

```
show ficonCUPzoning
```

Output

The data is presented as a table with the following properties:

FICON CUP Zoning State	The enabled state of the FICON CUP Zoning feature
Host Control List	List of 0-8 control hosts, displays "empty" for control host list with no members.

Output example

```
FICON CUP Zoning State:  Enabled
Host Control List
-----------------------
01:02:03:04:05:06:07:08
09:0A:0B:0C:0D:0E:0F:00
```

show.ficonMS

Syntax

```
ficonMs
```

Description

This command displays the FICON MS settings.

NOTE
This command is displayed on a Sphereon 3016 only if the feature key is installed.

Parameters

This command has no parameters.

Command example

```
Root> show ficonms
```

Output

The data is displayed as a table that includes the following properties:

Ficon MS State	The state of the FICON MS feature.
Ficon MIHPTO	The Ficon MIHPTO value in seconds.

Output example

```
Ficon MS State:              Disabled
Ficon MIHPTO (seconds):      180
```

show.frus

Syntax

```
frus
```

Description

This command displays information about all field-replaceable units (FRUs).

Parameters

This command has no parameters.

Command example

```
Root> show frus
```

Output

The FRU information is displayed as a table that includes the following properties:

FRU	The FRU name. (This may show *Unknown* or *Not Installed* if the FRU is not installed.) The QPM FRU is applicable only to Intrepid 6140.
Position	The relative position of the FRU, that is, its slot.
State	The state of the FRU. Values are: **Active**—the current module is active. **Backup**—this module is not currently being used, but it is available for immediate failover. **Degraded**—the back end path is failed. (QPM and XPM only). **Powered Off**—the module is installed, but powered off. (Intrepid 6064 and QPM only). **NotInst**—the module is not currently installed. **Failed**—the current module is failed.
Serial Num	The serial number of the FRU. (This field is blank for power supply modules of the Sphereon 4300 and Sphereon 4500 switches.)
Part Num	The part number of the FRU.
Beacon	The beaconing state of the FRU. Valid values are *On* or *Off*.
Pwr On Hrs	The power-on hours value for the FRU.

ATTENTION
The QPM FRU is only applicable to Intrepid 6140 and Intrepid 6064.

Output example

The output from the *show.frus* command displays as follows:

```
FRU    Position  State   Serial Num      Part Num   Beacon  Pwr On Hrs
-----  --------  ------  --------------  ---------  ------  ----------
CTP    0         Active  470-000399-700  123456789  False   2800
CTP    1         Backup  470-000399-700  223456789  True    2801
SBAR   0         Active  470-000399-700  223456789  False   2801
SBAR   1         Failed  470-000399-700  223456789  False   2801
FPM    0         Prwoff
FPM    1         Active  470-000399-700  223456789  False   2801
QPM    3         Active  470-000399-700  223456789  False   831
XPM    2         Degred  470-000399-700  223456789  False   831
UPM    4         Active  470-000399-700  223456789  False   831
Power  0         Active  470-000399-700  223456789  False   831
Fan    0         Active  470-000399-700  223456789  False   831
```

show.ip.ethernet

Syntax

```
ethernet
```

Description

This command displays Ethernet attributes.

Parameters

This command has no parameters.

Command example

```
Root> show ip ethernet
```

Output

The Ethernet attributes data is displayed as a table that includes the following properties:

IP Address	The IP address for the Ethernet adapter as set in the *config.ip.ethernet* command.
Gateway Address	The gateway address for the Ethernet adapter as set in the *config.ip.ethernet* command.
Subnet Mask	The subnet mask for the Ethernet adapter as set in the *config.ip.ethernet* command.

Output example

The output from the *show.ip.ethernet* command displays as follows:

```
LAN Information
IP Address:       144.49.10.15
Gateway Address:  144.49.10.1
Subnet Mask:      255.255.255.0
```

show.linkIncidentLog

Syntax

```
linkIncidentLog [clear]
```

Description

This command displays the contents of the link incident log on the director or switch.

NOTE
If the switch is restarted (as occurs during IPL, IML, configuration reset, feature key installation, or firmware load) or is power cycled, the information in the link incident log is lost.

Parameters

This command has one optional parameter:

clear	Whether all link incident log entries should be cleared.

Command example

```
Root> show linkIncidentLog
```

Output

The event log data are displayed as a table that includes the following properties:

Date/Time	The date and time when the event occurred.
Port	The number of the port where the link incident occurred.
Link Incident Event	An ASCII string describing the link incident event.

Output example

The output from the *show.linkIncidentLog* command displays as follows:

```
Date / Time       Port  Link Incident Event
---------------   ----  ------------------------------------------------------
02/27/03 01:28P   20    Not Operational primitive sequence (NOS) received.
02/27/03 01:28P   4     Primitive sequence timeout.
02/27/03 01:27P   62    Not Operational primitive sequence (NOS) received.
02/27/03 01:27P   62    Invalid primitive seq received for current link state
```

show.loginServer

Syntax

```
loginServer
```

Description

This command displays information from the login server database for devices attached to this switch. Note that it is possible to have more than one device per port for any public loop devices attached to an FL_Port.

Parameters

This command has no parameters.

Command example

```
Root> show loginServer
```

Output

The device information is displayed as a table that includes the following properties:

Port	The port number where the device is attached.
BB Crdt	The Buffer to buffer credit (BB_Credit). The maximum number of remaining frames that can be transmitted without causing a buffer overrun condition at the receiver.
RxFldSz	The buffer-to-buffer receive data field size from the FLOGI received from the attached N_Port.
COS	The class of service (for example, 1; 2; 3; 4; 5; 6; F; 1,2; 2,3).
Port Name	The port WWN of the attached device.
Node Name	The node WWN of the attached device.

Output example

The output from the *show.loginServer* command displays as follows:

```
Port BB Crdt  RxFldSz  COS  Port Name                Node Name
---- -------  -------  ---  -----------------------  -----------------------
0    10                2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
1    10                2    00:11:22:33:44:55:00:78  20:11:22:33:44:55:66:78
4    10                2,3  00:11:22:33:44:55:00:79  20:11:22:33:44:55:66:79
7    10                2,3  00:11:22:33:44:55:00:80  20:11:22:33:44:55:66:80
8    10                2    00:11:22:33:44:55:00:81  20:11:22:33:44:55:66:81
10   10                2,3  00:11:22:33:44:55:00:82  20:11:22:33:44:55:66:82
11   10                2,3  00:11:22:33:44:55:00:83  20:11:22:33:44:55:66:83
12   10                3    00:11:22:33:44:55:00:84  20:11:22:33:44:55:66:84
13   10                2,3  00:11:22:33:44:55:00:85  20:11:22:33:44:55:66:85
15   10                2,3  00:11:22:33:44:55:00:86  20:11:22:33:44:55:66:86
```

show.nameServer

Syntax

```
nameServer DID
```

Description

This command displays information from the name server database for devices attached to this switch when DID is not specified. If DID is specified, the local name server database entries for the specified domain are displayed. If the parameter is "all", then all of the name server database entries for all the domains in the fabric is displayed. Note that it is possible to have more than one device per port for any public loop devices attached to an FL_Port.

Parameters

This command has one optional parameter.

DID	The DID of the switch whose name server database information is to be displayed. This parameter can also be *all*.

Command example

```
Root> show nameServer
```

Output

The device information data is displayed as a table that includes the following properties:

DID	The DID of the switch whose name server entries are being displayed.
Type	The type of the port (*N*, *NL*, *F/NL*, *F*, *FL*, *E*, *B*).
Port Id	The 24-bit Fibre Channel address.
Port Name	The port WWN of the attached device.
Node Name	The node WWN of the attached device.
COS	The class of service (for example, 1; 2; 3; 4; 5; 6; F; 1,2; 2,3).
FC4 Types	The FC4 types registered for this device. One or more numbers display in this field. The numbers in this field correspond to the list at the bottom of the output example below. Note: There can be multiple FC4 types for each device. Since this is very rare, the CLI may wrap in the event that more than two are registered for this device.

Output example

The output from the *show.nameServer* command displays as follows:

```
Show> nameServer all

DID  Type  PortId  Port Name               Node Name               COS  FC4
---  ----  ------  ----------------------  ----------------------  ---  ---
1    F     613613  50:06:04:8A:CC:C8:61:51  50:06:04:8A:CC:C8:61:51
1    F     613B13  10:00:00:00:C9:20:DB:1F  20:00:00:00:C9:20:DB:1F
21   F     753713  50:06:04:8A:CC:C8:61:50  50:06:04:8A:CC:C8:61:50
28   F     7C3913  10:00:00:00:C9:20:DA:D1  20:00:00:00:C9:20:DA:D1
12   F     6C3A13  10:00:00:00:C9:20:DB:10  20:00:00:00:C9:20:DB:10

FC4 types decode information can be viewed via the show nameserverFC4Types CLI
command

Show> nameServer 1
```

```
DID  Type  PortId  Port Name                Node Name                COS  FC4
---  ----  ------  -----------------------  -----------------------  ---  ---
1    F     613613  50:06:04:8A:CC:C8:61:51  50:06:04:8A:CC:C8:61:51
1    F     613B13  10:00:00:00:C9:20:DB:1F  20:00:00:00:C9:20:DB:1F

FC4 types decode information can be viewed via the show nameserverFC4Types CLI
command

Show> nameServer

DID  Type  PortId  Port Name                Node Name                COS  FC4
---  ----  ------  -----------------------  -----------------------  ---  ---
28   F     7C3913  10:00:00:00:C9:20:DA:D1  20:00:00:00:C9:20:DA:D1

FC4 types decode information can be viewed via the show nameserverFC4Types CLI
command
Show> nameServer 15 (15 is not in the fabric)
No entries in the database for Domain 15.
```

show.nameServerExt

Syntax

```
nameServerExt
```

Description

This command displays extended information from the name server database for devices attached to this switch. The command provides symbolic name server information, as well as the same information as the *show.nameServer* command. Multiple devices per port are possible for any public loop device attached to an FL_Port.

NOTE

Because it contains symbolic name server information that can be lengthy, the CLI output wraps several times per node. For this reason, this command is supported only in comma-delimited mode. For more information about the comma-delimited mode, see "Using the commaDelim command" on page 15.

Parameters

This command has no parameters.

Command example

```
Root> show nameServerExt
```

Output

The device information data is displayed as a table that includes the following properties:

Type	The type (N, NL, F/NL, F, FL, E, B).
Port Id	The 24-bit Fibre Channel address.
Port Name	The port WWN of the attached device.
Node Name	The node WWN of the attached device.
COS	The class of service (for example, 1; 2; 3; 4; 5; 6; F; 1,2; 2,3).
FC4	The FC4 types registered for this device. One or more numbers display in this field. The numbers in this field correspond to the list in the output example for "show.nameServer" on page 239.
SymNodeName	255-character representation of the Symbolic Node Name.
SymPortName	255-character representation of the Symbolic Port Name.

Output example

The output from the *show.nameServerExt* command displays as follows:

```
Type, Port Id, Port Name, Node Name, COS, FC4 Types, SymNodeName, SymPortName,
N,  010400, 00:11:22:33:44:55:00:77, 20:11:22:33:44:55:66:77, 2-3, 2, Node Name A,
Port Name A,
N,  010500, 00:11:22:33:44:55:01:77, 20:11:22:33:44:55:66:77, 2-3, 0, This Is
Symbolic Node Name B, Symbolic Port Name B Is Slightly Longer
N, 010600, 00:11:22:33:44:55:66:02, 20:11:22:33:44:55:66:77, 2-3, 2, , ,
FL, 000001, 00:11:22:33:44:55:66:03, 20:11:22:33:44:55:66:77, 2, 0, Loop Node 1,
Loop Port 7
FL, 000002, 00:11:22:33:44:55:66:04  20:11:22:33:44:55:66:77, 3, 2, Loop Node 2,
Loop Port 7,
```

show.nameServerFC4Types

Synopsis

```
nameServerFC4Types
```

Description

This command displays the FC4 types.

One or more FC4 types are displayed in the FC4 field from the name server command. These FC4 types index into the list of FC4 types in the table. Some of the valid FC4 types are displayed in the following *Output example*.

Parameters

This command has no parameters.

Command example

```
Root> show nameServerFC4Types
```

Output example

```
Show> nameserverFC4Types
0. ISO/IEC 8802-2 LLC
1. ISO/IEC 8802-2 LLC/SNAP
2. SCSI-FCP
3. SCSI-GPP
4. IPI-3 Master
5. IPI-3 Slave
6. IPI-3 Peer
7. CP IPI-3 Master
8. CP IPI-3 Slave
9. CP IPI-3 Peer
10. SBCCS-Channel
11. SBCCS-Cntrl Unit
12. FC Srvcs
13. FC-FG
14. FC-XS
15. FC-AL
16. SNMP
17. HIPPI-FP
18. Vendor Unique
```

show.NPIV.config

Syntax

```
config
```

Description

This command displays the current NPIV configuration for all ports.

NOTE
The command “config.NPIV.show” on page 46 has functionality that is identical to this command.

Parameters

This command has no parameters.

Command example

```
Root> show NPIV config
```

Output

This command displays the following NPIV configuration data:

NPIV state	The current enabled/disabled state of the NPIV feature.
Max Allowed NPIV Login Table	A table mapping each port number on the switch to a corresponding max number of NPIV logins setting.

Output example

```
NPIV state:  Enabled
Port   Max Allowed NPIV Logins
----   ----------------------
1      10
2      10
3      10
4      0
5      0
7      130...
```

show.openSysMS.config

Syntax

```
config
```

Description

This command displays the Open System Management Server (OSMS) state and the Open System Management Server Host Control State.

Parameters

This command has no parameters.

Command example

```
Root> show openSysMS config
```

Output

The configuration data is displayed as a table that includes the following properties:

openSysMS State	The Open System Management Server state.
Host Control State	The Open System Management Server Host Control state.

Output example

```
openSysMS State:    disable
Host Control State: enable
```

show.openSysMS.platformInfo

Synopsis

```
platformInfo type [name]
```

Description

This command is used to query the OSMS to find the status of the platform registration process.

Parameters

This command has two parameters. The second parameter is optional.

type	The type of query. Valid query types are: *GPNL – Get Platform Name List* *GPLNL – Get Platform Node Name List for a particular platform* *GPLML – Get Platform Management Address List for a particular platform* *GPLT – Get Platform Type for a particular platform*
name	The platform name. It is a required parameter for *GPLNL*, *GPLML* and *GPLT* queries. There is no name parameter for *GPNL* query.

Command example

```
Root> show openSysMS platformInfo GPNL
```

Output

The configuration data is displayed as a table that includes the following properties:

Platform Name	The list of Platform Name List for GPNL query.
Node Name	The list of Platform Node Name List for GPLNL queries.
Platform Management Address	The Platform Management Address (URL) List for GPLML queries.
Platform Type	The Platform Type for GPLT queries.

Output example

```
show.openSysMS>platformInfo GPNL
```

```
Platfrom Name
-------------------------
Platform 1
Platform 2
Platform 3

show.openSysMS>platformInfo GPLNL "platform 2"
Node Name
-----------------------------------
Node name 1
Node name 2

show.oOpenSysMS>platformInfo GPLML "platform 1"
Platform Management Address
--------------------------------
Management Address #1
Management Address #2
show.openSysMS>platformInfo GPLT "platform 3"

Platform Type
-------------
00 00 00 0A
```

show.openTrunking.config

Syntax

```
config
```

Description

This command displays the trunking configuration for all ports.

Parameters

This command has no parameters.

Command example

```
show openTrunking config
```

Output

The device information is displayed as a table that includes the following:

Unresolved Congestion	The current enabled/disabled state of the unresolved congestion trunking feature.
Backpressure	The current enabled/disabled state of the backpressure trunking feature.
Low BB_Credit Threshold	The current threshold setting of the low BB_Credit threshold trunking feature listed as a percentage. If this value is configured to be the default, `(default)` is displayed alongside the threshold value. The default value is 75%.
Congestion Threshold Table	A table mapping each port number on the switch to a corresponding threshold setting. The threshold is listed as a percentage. If this value is configured to be the default, `(default)` is displayed alongside the threshold value. The default value is 60%.

Output example

The output from the *show.openTrunking.config* command displays as follows:

```
Unresolved Congestion:            Enabled
Backpressure:                     Disabled
Low BB_Credit Threshold (%):      75 (default)
Port  Threshold %
----  ------------
1     60 (default)
2     69
3     60 (default)
4     60 (default)
5     90
6      80
...
```

show.openTrunking.rerouteLog

Syntax

```
reroutelog [clear]
```

Description

This command displays the Open Trunking Reroute Log information.

NOTE
If the switch is restarted (as occurs during IPL, IML, configuration reset, feature key installation, or firmware load) or is power cycled, the information in the Open Trunking Reroute Log is lost.

Parameters

This command has one optional parameter:

clear	Whether all reroute log entries should be cleared.

Command example

```
show opentrunking reroutelog
```

NOTE
The *clear* parameter also clears the log entries for your SAN management application.

Output

The device information data is displayed as a table that includes the following properties:

Date/Time	The date/time when the rerouting event occurred.
Rcv	The port associated with the flow that was rerouted.
Dom	The target domain associated with the flow that was rerouted.
Old	The exit port number on this switch that the flow used to get to the target domain.
New	The exit port number on this switch that the flow now uses to get to the target domain.

Output example

The output from the *show.opentrunking.reroutelog* command displays as follows:

```
Date/Time        RcvPort  Dom  OldExit  NewExit  ---------------  -------  ---
-------  -------    04/12/01 10:58A  63       2    41       42
03/23/02 12:01P  4        3    35       36
```

show.port.config

Syntax

```
config
```

Description

This command shows the port configuration for all ports.

Parameters

This command has no parameters.

Command example

```
Root> show port config
```

Output

The port configuration attributes are displayed as a table that includes the following properties:

Port	The port number.
Name	The name of the port as set in the *config.port.name* command.
Blocked	The blocked state of the port as set in the *config.port.blocked* command.
FAN	The configured Fabric Address Notification (FAN) state. (Sphereon 4300, Sphereon 4500, Sphereon 4400, and Sphereon 4700 switches only).
Type	The port type as set in the *config.port.type* command.
Speed	The configured port speed. *1G – 1 Gb/sec* *2G – 2 Gb/sec* *4G – 4 Gb/sec (Sphereon 4400 and Sphereon 4700 only)* *10G – 10 Gb/sec (XPM only)* *Neg – Negotiate* *4G Sust – 4 Gb/sec Sustained (QPM only)* *4G Burst – 4 Gb/sec Burst (QPM only)* *Neg Sust – Negotiate Sustained (QPM only)* *Neg 2G Max – Negotiate 2 Gb/sec Maximum (QPM only)* *Neg B 4G Max – Negotiate Burst 4 Gb/sec Maximum (QPM only)*
Rx Crdts	The number of Rx BB_Credits as set in the *config.port.rxCredits* command.

Output example

The output from the *show.port.config* command displays as follows:

```
Port  Name                      Blocked    Type    Speed            Rx Crdts
----  ------------------------  ---------  ------  ---------------  --------
0     port_0_name               Blocked    gxPort  Neg Sust         12
1                               Blocked    gxPort  Neg Burst        12
2                               Blocked    gxPort  Neg Burst        12
3                               Blocked    gxPort  Neg Burst        12
...
```

show.port.exit

Syntax

```
exit destDomainID sourcePort
```

Description

This command displays the exit port from a source port to a given destination domain. This command shows the preferred path configuration.

Use *all* for one of the command's parameters to display all configured and actual exit ports for either the destination domain ID or the specified source port. You cannot specify *all* for both parameters. If the destination domain is set to *all*, then all paths from the specified source port are displayed. If the source port is set to *all*, the output shows all source port paths to the specified domain.

Parameters

This command has the following parameters:

destDomainId	The destination domain ID. Valid domain IDs are in the range 1–31, or, use *all* to show all exit ports to and from the source port specified in the sourcePort parameter.
sourcePort	The number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 4700 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or, you can specify *all* to show all exit ports to the destination domain ID specified for the *destDomainId* parameter.

Output

The output from *show.port.exit* includes the following parameters:

Destination Domain	The destination domain ID to which a preferred path has been configured. This is displayed only if the destination domain parameter is set to *all*.
Source Port	The source port for which a preferred path to the specified destination domain ID is specified. This is displayed only if the source port parameter is set to *all*.
Exit Port	This is the actual exit port being used for the given path. The value *No Domain* displays when the destination domain doesn't exist in the fabric. The value *No Source* displays when the source port is in an offline state. The value *Fabric Building* displays when the fabric is still building.

Command and output examples

The following examples show the output returned by the three methods of specifying the *show.port.exit* command.

Output with single values for both parameters

```
Root> show port exit 21 10
Exit Port:  45
```

Output with destDomainId set to all

```
Root> show port exit all 15
Destination Domain  Exit Port
------------------  ----------------
1                   23
2                   No Domain
3                   23
…
31                  No Domain
```

Output with sourcePort set to all

```
Root> show port exit 1 all
Source Port         Exit Port
------------------  ----------------
0                   No Source
1                   5
2                   No Source
3                   6
…
```

show.port.info

Syntax

```
info
```

Description

This command displays port information for all ports.

Parameters

This command has no parameters.

Command example

```
Root> show port info
```

Output

The port information data is displayed as a table that includes the following properties:

Port	The port number.
WWN	The WWN of the port.
OpSpeed	The current operating speed. Valid values are: *Not Established* *1G – 1 Gb/sec* *2G – 2 Gb/sec* *4G – 4 Gb/sec (Sphereon 4400 and Sphereon 4700 only)* *10G – 10 Gb/sec (XPM only)* *4G Sust – 4 Gb/sec Sustained (QPM only)* *4G Burst – 4 Gb/sec Burst (QPM only)* *For QPM inactive port, it displays "Supports Port number (note: the sustained port number)"*
SpeedCap	The current transceiver capability speed. Valid values are: *1 – 1g* *2 – 2g* *4 – 4g capable (Sphereon 4400 and Sphereon 4700 only)* *Neg – Negotiable speed* *Neg_2 – Negotiable speed up to 2g maximum* *4_B – 4g Burst* *4_S – 4g Sustained* *Neg_S – Negotiable speed in sustained mode* *Neg_B_4 – Negotiable speed in burst mode up to 4g maximum*

Output example

The output from the *show.port.info* command displays as follows:

```
Port  WWN                      OpSpeed    SpeedCap
----  -----------------------  ---------  ---------------------------------------
0     20:10:08:00:88:04:9A:1B  Neg        1  2  4_S  4_B  Neg_S  4_S
1     20:11:08:00:88:04:9A:1B  1          1  2  4_B  Neg_S
2     20:12:08:00:88:04:9A:1B  Neg        1  2  4_S  4_B  Neg_S  Neg_2_Max
3     20:13:08:00:88:04:9A:1B  1          1  2  4_B  Neg_S
4     10:00:80:04:11:22:33:44  2          1  2  Neg
5     10:00:80:05:11:22:33:44  2          1  2  Neg
6     10:00:80:06:11:22:33:44  2          1  2  Neg
7     10:00:80:07:11:22:33:44  2          1  2  Neg
8     10:00:80:08:11:22:33:44  2          1  2  Neg
9     10:00:80:09:11:22:33:44  2          1  2  Neg
10    10:00:80:10:11:22:33:44  1          1  2  Neg
11    10:00:80:11:11:22:33:44  1          1  2  Neg
12    10:00:80:12:11:22:33:44  1          1  2  Neg
13    10:00:80:13:11:22:33:44  1          1  2  Neg
14    10:00:80:14:11:22:33:44  1          1  2  Neg
15    10:00:80:15:11:22:33:44  1          1  2  Neg
```

show.port.nodes

Syntax

```
nodes portNumber
```

Description

This command displays the login server entries for a specified port. This command is valid only on the Sphereon 4300 and Sphereon 4500 switches.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 4700

Command example

```
Root> show port nodes portNumber
```

Output

The port nodes data is displayed as a table that includes the following properties:

FC Addr	The Fibre Channel address of nodes attached to this port. Private devices are assigned address strings of 0000 followed by the two-digit hexadecimal Arbitrated Loop Physical Address (AL_PA), instead of the 6 digit hexadecimal number presented for public devices.
BB Crdt	The maximum number of outstanding frames which can be transmitted without causing a buffer over-run condition at the receiver.
RxFldSz	Buffer-to-buffer Receive Data Field Size from the FLOGI received from the attached N_Port.
COS	Class of service: 1; 2; 3; 4; 5; 6; F; 1,2; 2,3...
Port Name	The port worldwide name of the attached device.
Node Name	The node worldwide name of the attached device.

Output example

The *show.port.nodes* command output for a mix of public and private nodes on a loop displays as follows:

```
FCAddr  BB Crdt  RxFldSz  COS  Port Name                Node Name
------  -------  -------  ---  -----------------------  -----------------------
612902  10               2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
612903  10       2112    2    00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
612904  10               2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
612905  10               2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
6129AB  8        2112    2    00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
6129AC  10               2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
6129AD  8                2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
6129AE  10               3    00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
6129FD  10               2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
6129FE  10               2,3  00:11:22:33:44:55:00:77  20:11:22:33:44:55:66:77
```

show.port.opticData

Syntax

```
opticData portNumber
```

Description

This command shows the overall optic health, enhanced digital diagnostic data, and the thresholds for the specified port. At the end of this display, it shows which measurements have exceeded their thresholds.

Parameters

This command has one parameter.

portNumber	The port number whose data is displayed. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the Sphereon 4700 0–63 for the Intrepid 6064 0–143 for the Intrepid 6140 (128–131 are inaccessible)

Command example

```
Show.Port> opticData 5
```

Output

This command displays the following optic data:

Type	The measurement type. Temperature is in celsius, voltage is in volts, power is in mW, and current is in mA.
Value	The value of the measurement.
Low Warning	The lower limit for the warning threshold.
High Warning	The higher limit for the warning threshold.
Low Alarm	The lower limit for the alarm threshold.
High Alarm	The higher limit for the alarm threshold.

Output example

The output from the *show.port.opticData* command displays as follows:

```
Port Number:    5
Overall Health: Alarm
Transceiver:    SFP
Type         Value    Low Warning  High Warning  Low Alarm  High Alarm
-----------  -------  -----------  ------------  ---------  ----------
Temperature  134.600  -40.000      100.000       -45.000    105.000
3.3 Voltage  3.290    3.000        3.600         2.900      3.700
Current      7.460    4.600        14.800        3.100      20.000
TX Power     400.000  112.000      398.000       89.000     501.000
RX Power     17.000   13.000       1000.000      4.000      1259.000
1.8 Voltage  N/A      N/A          N/A           N/A        N/A
5.0 Voltage  N/A      N/A          N/A           N/A        N/A

Temperature High Alarm
TX Power High Warning
```

show.port.opticEDD

Syntax

```
OpticEDD
```

Description

This command displays Enhanced Digital Diagnostics (EDD) information for all ports. This information is in HEX format. If there is no port connected then “Unk” is displayed. For ports that are connected and does not support predictive optics monitoring feature displays “Unknown”.

Parameters

This command has no parameters.

Command example

```
Show port opticEDD
```

Output

The port optic diagnostic data is displayed as a table that includes the following properties.

Port	The port number.
Xcvr	The transceiver type.
Temp	The optic temperature in celsius.
3.3 Voltage	The 3.3 voltage in volts.
Current	The current in mA.
TX Pwr	The transceiver power in uW.
RX Pwr	The receiver power in uW.
1.8 Voltage	The 1.8 voltage in volts.
5.0 Voltage	The 5.0 voltage in volts.

Output example

The *show.port.opticEDD* command output displays as follows:

```
Port   Xvr    Temp   3.3 Volt   Current    TX Power   RX Power   1.8 Volt5.0 Volt
----   ---    -----  --------   -------    ---------  ---------  --------   -------
0      UNK    UnknownUnknown    Unknown    Unknown    Unknown    UnknownUnknown
1      UNK    UnknownUnknown    Unknown    Unknown    Unknown    UnknownUnknown
2      UNK    UnknownUnknown    Unknown    Unknown    Unknown    UnknownUnknown
3      UNK    UnknownUnknown    Unknown    Unknown    Unknown    UnknownUnknown
4      XFP    36.105 3.256      5.324      602.100    289.3001.779  4.998
```

show.port.opticHealth

Syntax

```
opticHealth
```

Description

This command shows the overall optic health for all ports that support Enhanced Digital Diagnostics (EDD).

NOTE
At unit startup, the health of the optics is read at roughly one optic per second, and once it reaches the last port, it starts from the beginning and updates any changes.

Parameters

This command has no parameters.

Output

This command displays the following optic data:

Port	The port number.
Overall Health	The overall health of the optic. Possible values are list below according to priority.
Alarm	One or more alarm threshold has been exceeded.
Warning	One or more warning threshold has been exceeded.
Normal	All measurements are within thresholds.
No Info	The optic does not support enhanced digital diagnostics or the state has not been updated yet.

NOTE
If both an *Alarm* and a *Warning* threshold have exceeded, then the *Alarm* state is displayed because it is of high priority.

Command example

```
Root> Show Port opticHealth
```

Output example

The *show.port.opticHealth* command output displays as follows:

```
Port  Transceiver  Overall Health
----  -----------  --------------
0     XPM          Normal
1     (Unaddressable)
2     (Unaddressable)
3     (Unaddressable)
4     SFP          Normal
5     Unk          No Info
6     Unk          No info
7     SFP          Warning
8     SFP          Alarm
...
```

show.port.opticInfo

Syntax

```
OpticInfo
```

Description

This command displays information about the optic.

Parameters

This command has no parameters.

Command example

```
Root> show port opticInfo
```

Output

The port optic data is displayed as a table that includes the following properties:

Port Number	The port number.
Transceiver	The transceiver type.
Vendor Name	The vender name.
Serial Number	The serial number.
Part Number,	The part number.
Revision Level	The revision level.
Supported Link Length	The Supported link length.
Extended Identifier	The extended identifier.
Date and Lot	The data and lot.

Output example

The *show.port.opticInfo* command output displays as follows:

```
Port Number,Tranceiver,Vendor Name,Serial Number,Part Number,Revision
Level,Supported Link Length,Extended Identifier,Date and Lot#,
0,SFP,E2O COMMS INC   ,36U1348         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
1,SFP,E2O COMMS INC   ,36U3682         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/04/03 Lot#   ,
2,SFP,E2O COMMS INC   ,36U1343         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
3,SFP,E2O COMMS INC   ,36U1344         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
4,SFP,E2O COMMS INC   ,36U1349         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
5,SFP,E2O COMMS INC   ,36U1346         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
6,SFP,E2O COMMS INC   ,35C6334         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,05/24/03 Lot#   ,
7,SFP,E2O COMMS INC   ,36U3677         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/04/03 Lot#   ,
```

```
8,SFP,E2O COMMS INC   ,36U1350         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
9,SFP,E2O COMMS INC   ,35D2220         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,05/16/03 Lot#   ,
10,SFP,E2O COMMS INC   ,36U1345         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
11,SFP,E2O COMMS INC   ,36U3681         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/04/03 Lot#   ,
12,SFP,E2O COMMS INC   ,3770978         ,EM212-LP3TA-MT  ,4R  ,0   0   30
15,4,07/09/03 Lot#   ,
13,SFP,E2O COMMS INC   ,36U1338         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
14,SFP,E2O COMMS INC   ,36U1347         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
15,SFP,E2O COMMS INC   ,36U1332         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
16,SFP,E2O COMMS INC   ,36U3676         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/04/03 Lot#   ,
17,SFP,E2O COMMS INC   ,476PM46         ,EMA2G-LD3TA-MT  ,2   ,0   0   30
15,4,07/07/04 Lot#   ,
18,SFP,E2O COMMS INC   ,3161215         ,EM212-LP3TA-MB  ,4   ,0   0   30
15,4,01/16/03 Lot#   ,
19,SFP,E2O COMMS INC   ,477P560         ,EMA2G-LD3TA-MT  ,2   ,0   0   30
15,4,07/08/04 Lot#   ,
20,SFP,E2O COMMS INC   ,36U1331         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
21,SFP,E2O COMMS INC   ,36U1335         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
22,SFP,E2O COMMS INC   ,36U1339         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#   ,
23,SFP,E2O COMMS INC   ,36U1341         ,EM212-LP3TA-MT  ,4   ,0   0   30
15,4,07/03/03 Lot#
```

show.port.profile

Syntax

```
show port profile
```

Description

This command displays the port configuration for the specified port.

Parameters

This command has one parameter:

portNumber	The port number. Valid values are: 0–15 for the Sphereon 3016 0–16 for the Sphereon 4400 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–32 for the Sphereon 4700 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command example

```
Root> show port profile portNumber 138
```

Output

The port profile information is displayed as a single output for an individual port.

Port Number	The port number.
Name	The configured port name.
Blocked	The blocked state. Valid values are true and false.
Blocked Reason	The blocked reason. Valid values are "*Blocked temporarily, Internal*","*Blocked by user*","*Blocked by hardware type change*","*Blocked by port fencing*".
Operating Type	The operating port type.
Operating Speed	The operating port speed. Valid values are *Not Established* *1G – 1 Gb/sec* *2G – 2 Gb/sec* *4G – 4 Gb/sec (Sphereon 4400 and Sphereon 4700 only)* *10G – 10 Gb/sec (XPM only)* *4G Sust – 4 Gb/sec Sustained (QPM only)* *4G Burst – 4 Gb/sec Burst (QPM only)* *For QPM inactive port, it displays "Supports Port number (note: the sustained port number)"*
Port WWN	The port WWN.
Configured Type	The configured port type.
Configured Speed	The configured port speed. *1G - 1 Gb/sec* *2G - 2 Gb/sec* *4G - 4 Gb/sec (Sphereon 4400 and Sphereon 4700 only)* *10G - 10 Gb/secGb/sec (XPM only)* *Neg - Negotiate* *4G Sust - 4 Gb/sec Sustained (QPM only)* *4G Burst - 4 Gb/sec Burst (QPM only)* *Neg Sust - Negotiate Sustained (QPM only)* *Neg 2G Max - Negotiate 2 Gb/sec Maximum (QPM only)* *Neg B 4G Max - Negotiate Burst 4 Gb/sec Maximum (QPM only)*
Beaconing	The beaconing state.
FAN	The FAN state.
FC Address	The Port Fibre Channel address.
Attached WWN	The node WWN of the device at the remote end of the link. A loop port displays the first attached loop device.
Operational State	The operational state of the port.

Reason	The reason that the port operational state is not “online”.
Rx BB_Credits	Then number of configured Rx BB_Credits.
Connector Type	The optic connector type.
Transceiver	The optic transceiver type.
Distance Capability	The optic distance capability.
Media Type	The optic media type.
Speed Capability	The optic speed capability.
10G FC Compliance	The optic 10G FC Compliance code.

Output example

The output from the *show.port.profile* command displays as follows:

```
Port Number:           4
Name:                  Sam's tape drive
Blocked:               False
Blocked Reason:
Operating Type:        FL Port
Operating Speed:       2G
Port WWN:             A2:33:15:C3:3F:00:00:0A
Configured Type:        Gx_Port
Configured Speed:      Neg
Beaconing:             Disabled
FAN:                   Disabled
FC Address:            034FA2
Attached WWN:          F0:01:02:A1:B0:22:00:12
Operational State:     Online
Reason:                None
Rx BB_Credits:         12
Connector Type:        LC
Transceiver:           Long LC
Distance Capability:   Long
Media Type:            M-M 50um
Speed Capability:      2 Gb/sec
10G FC Compliance:     None
```

show.port.showPortAddr

Syntax

```
showPortAddr
```

Description

This command displays the port address configuration for all ports.

NOTE
The “config.port.showPortAddr” on page 56 has functionality that is identical to this command.

Parameters

This command has no parameters.

Command example

```
Root> show port showPortAddr
```

Output

The port configuration is shown as a table of properties. The following properties are displayed:

Port	The port number.
Original Addr	The original port address of the port.
Current Addr	The current port address of the port.
Swapped Port Num	If the port is swapped with another port, it displays the port number of the port it is swapped with.

Output example

```
Port   Original Addr     Current Addr  SwappedPort Num
----   -------------     ------------  ---------------
0      4                 4
1      5                 5
2      6                 7             3
3      7                 6             2
4      8                 8
5      9                 9
6      a                 a
7      b                 b
8      c                 c
...
```

show.port.status

Syntax

```
status
```

Description

This command displays port status for all ports.

Parameters

This command has no parameters.

Command example

```
Root> show port status
```

Output

The port status data is displayed as a table that includes the following properties:

Port	The port number.
State	The port state (for example, Segmented E_Port, Invalid Attachment, Not Installed, Online, Offline, Not Operational, No Light, Testing, Port Failure, Link Reset, or Inactive).
Type	The operational port type. If the configured port type is F_Port or E_Port, this value will match the configured type. If the configured type is G_Port, this value can be E_Port, F_Port, or G_Port, depending on what is connected to the port. On the Sphereon 4300 and Sphereon 4500, if the configured port type is Fx_Port, the operational port type can include FL_Port in addition to the values noted above for F_Port. If the configured port type is Gx_Port, then the operational port type can include FL_Port in addition to the values noted above for G_Port.
Attached WWN	The WWN of the device or switch attached to the port, if one is attached.

Beaconing	The beaconing state for the port (Off or On).
Reason	An optional message number that indicates whether the port has a segmented ISL, if a port binding violation has occurred, or if the port is inactive. The message description for this message number is provided at the bottom of the table. If the operational state is *Segmented E_Port*, only the following messages can be generated: 01: Segment Not Defined 02: Incompatible Operating Parameters 03: Duplicate Domain ID(s) 04: Incompatible Zoning Configurations 05: Build Fabric Protocol Error 06: No Principal Switch 07: No Response from Attached Switch 08: ELP Retransmission Failure Timeout If the operational state is *Invalid Attachment* only the following messages can be generated: 09: Unknown 10: ISL connection not allowed on this port 11: ELP rejected by the attached switch 12: Incompatible switch at other end of the ISL 13: External loopback adapter connected to the port 14: N_Port connection not allowed on this port 15: Non-McDATA switch at other end of the ISL 16: ISL connection not allowed on this port 17: ISL connection not allowed to external Fabrics 18: Port binding violation - unauthorized WWN 19: Unresponsive Node Connected to Port 20: Incompatible security attributes 21: Fabric Binding violation 22: Authorization failure 23: Switch Binding violation
Reason (cont.)	If the operational state is *Inactive* only the following messages can be generated: 24: Inactive - RC 0 25: No Serial Number 26: Feature Not Enabled 27: Switch Speed Conflict

Output example

The output from the *show.port.status* command displays as follows:

```
Port State              Type   Attached WWN             Beaconing  Reason
---- -----------------  -----  -----------------------  ---------  ------
0    Online             fPort  10:00:80:00:11:22:33:44  Off
1    Online             gPort  10:00:80:00:11:22:33:45  On
2    No Light           fPort  10:00:80:00:11:22:33:55  On
3    Offline            ePort  10:00:80:00:11:22:33:00  Off
4    Online             gPort  10:00:80:00:11:22:33:57  Off
```

```
5    Port Failure       fPort  10:00:80:00:11:22:33:46  Off
6    Link Reset         gPort  10:00:80:00:11:22:33:63  Off
7    Segmented E_Port   ePort  10:00:80:00:11:22:33:47  Off        02
8    Online             ePort  10:00:80:00:11:22:33:88  Off
9    Offline            fPort  10:00:80:00:11:22:33:49  Off
10   Inactive           ePort  10:00:80:00:11:22:33:50  Off        26
11   Online             fPort  10:00:80:00:11:22:33:53  Off
12   No Light           fPort  10:00:80:00:11:22:33:56  Off
13   Online             fPort  10:00:80:00:11:22:33:59  Off
14   Invalid Attachment fPort  10:00:80:00:11:22:33:64  Off        15
15   Online             fPort  10:00:80:00:11:22:33:66  Off

02: Duplicate Domain ID(s)
03: Switch Speed Conflict
07: ISL connection not allowed on this port
```

show.port.technology

Syntax

```
technology
```

Description

This command displays port technology information for all ports.

Parameters

This command has no parameters.

Command example

```
Root> show port technology
```

Output

The port technology data is displayed as a table that includes the following properties:

Port	The port number.
Connectr	The port connector type (LC, MT_RJ, MU, Internal).
Transcvr	The transceiver type (Long LC, Short, Short OFC, Long LL, Long Dist).
Distance	The distances supported (Short, Intermediate, Long, Very Long).
Media	The media type (M-M 62.5um, M-M 50um, M-M 50,62.5um, S-M 9um, Copper).

Output example

The output from the show.port.technology command displays as follows:

```
Port Connectr Transcvr  Distance     Media
---- -------- --------- ------------ -----------
0    LC       Long LC   Long         M-M 50um
1    LC       Long LC   Long         M-M 50um
2    LC       Long LC   Long         M-M 50um
3    MT_RJ    Long LC   Long         M-M 50um
4    MT_RJ    Long LC   Long         M-M 50um
5    MT_RJ    Long LC   Long         M-M 50um
6    LC       Long LC   Long         M-M 50um
7    LC       Long LC   Long         M-M 50um
8    LC       Long LC   Long         M-M 50um
9    LC       Long LC   Long         M-M 50um
10   LC       Long LC   Long         M-M 50um
11   LC       Long LC   Long         M-M 50um
12   LC       Long LC   Long         M-M 50um
13   LC       Long LC   Long         M-M 50um
14   LC       Long LC   Long         M-M 50um
15   LC       Long LC   Long         M-M 50um
```

show.preferredPath.showPath

Syntax

```
showPath destDomainID sourcePort
```

Description

This command displays the specified preferred path configuration and the actual path used by the system. The output shows both the exit port as configured for the preferredPath feature and the actual exit port currently being used for traffic.

Use *all* for one of the command's parameters to display all configured and actual exit ports for either the destination domain ID or the specified source port. You cannot specify *all* for both parameters. If the destination domain is set to *all*, all paths from the specified source port are displayed. If the source port is set to *all*, the output shows all source port paths to the specified domain.

Parameters

This command has the following parameters:

destDomainId	The destination domain ID. Valid domain IDs are in the range 1–31 or *all*, which shows all paths to and from the source port specified in the sourcePort parameter.
sourcePort	The number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–15 for the Sphereon 4400 0–23 for the Sphereon 4500 0-31 for the Sphereon 4700 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or, you can specify *all* to show all paths to the destination domain ID specified for the destDomainId parameter.

Output

The output from the *show.preferredPath.showPath* command includes the following parameters:

Destination Domain	The destination domain ID to which a preferred path has been configured. This is displayed only if the destination domain parameter is set to *all*.
Source Port	The source port for which a preferred path to the specified destination domain ID is specified. This is displayed only if the source port parameter is set to *all*.
Preferred Exit Port	The configured preferred path exit port. This value can be any port number, or blank to indicate that no preferred path has been configured.
Actual Exit Port	The actual exit port being used for the given path.

Command and Output examples

The following examples show the output returned by the three methods of specifying the *show.preferredPath.showPath* command.

Single values for both parameters

```
Root> show preferredPath showPath 21 10
Preferred Path State: Enabled
Preferred Exit Port:  Not Configured
Actual Exit Port:     45
```

destDomainId set to all

```
Root> show preferredPath showPath all 15
Preferred Path State: Enabled
```

```
Destination Domain  Preferred Exit Port  Actual Exit Port
------------------  -------------------  ----------------
1                   23                   23
3                   24                   No Path
4                   23                   23
17                  12                   No Source
```

sourcePort set to all

```
Root> show preferredPath showPath 1 all
Preferred Path State: Enabled
Source Port         Preferred Exit Port  Actual Exit Port
------------------  -------------------  ----------------
0                   2                    No Source
2                   5                    5
3                   17                   No Path
22                  5                    6
```

show.preferredPath.showState

Syntax

```
showState
```

Description

This command displays the state of the preferred path.

Parameters

This command has one parameter:

Preferred Path State	The enabled/disabled state of the preferred path.

Command example

```
Root> show.preferredPath.showState
```

show.security.fabricBinding

Syntax

```
fabricBinding
```

Description

This command displays the fabric binding configuration saved on the fabric. The command performs the same function as the command “config.security.fabricBinding.showActive” on page 85.

Parameters

This command has no parameters.

Command example

```
Root> show security fabricBinding
```

Output

The fabric binding configuration data is displayed as a table that includes the following properties:

Domain ID	The domain ID of the Fabric Binding Membership List (FBML) member. Valid domain IDs range from 1 to 239.
WWN	The world wide name (WWN) of the FBML member in colon-delimited hexadecimal notation.
Attachment Status	Whether the FBML member is Local, Attached, or Unattached. For more information, see "Fabric Binding membership terminology" on page 81.

Output example

The output from the *show.security.fabricBinding* command displays as follows:

```
Domain 1  (20:30:40:50:60:70:8F:1A) (Local)
Domain 3  (00:11:22:33:44:55:66:77) (Unattached)
Domain 2  (88:99:AA:BB:CC:DD:EE:FF) (Attached)
Domain 14 (11:55:35:45:24:78:98:FA) (Attached)
```

show.security.log

Syntax

```
log [clear]
```

Description

This command shows the contents of the security log as maintained in NV-RAM on the director or switch.

Parameters

This command has one parameter:

clear	Whether all security log entries should be cleared.

Command example

```
Root> show security log
```

Output

The security log data are displayed as a table that includes the following properties:

Reason	The reason code for the security event.
Date/Time	The date and time when the event occurred.
Trigger Level	The trigger level of the event. Possible values are *Informational, Security Change, or Error.*
Category	The event category message. Possible values are *Successful Connection, Disconnection, Configuration Change, Authorization Failure, Authentication Failure, or Reserved.*
Count	A cumulative count of events within a known period.
Desc	A formatted string containing a description of the event.
Data	A formatted string containing additional or event-specific data.

Output example

The output from the *show.security.log* command displays as follows:

```
Reason  Date/Time        Trigger Level    Category                Count
------  ---------------  ---------------  ----------------------  -----
10000   04/12/01 10:58A  Informational    Successful Connection   375
  Desc: EWS User Connected
  Data: Usr=Administrator IPaddr=001.002.003.004 Role=admin
10305   04/11/01 01:03A  Error            Authorization Failure   1
  Desc: IP Access Control List Violation
  Data: IPaddr=172.072.016.097 SrcPort=0072 DestPort=0124
10300   04/02/01 08:30P  Error            Authorization Failure   3
  Desc: Fabric Binding Mismatch
  Data: Prt=0100 NbrW=02:15:F4:2A:11:0F:11:00 NbrDID=004 ErrDID=001
10411   03/31/01 02:24A  Error            Authentication Failure  1
  Desc: OS Management Server Authentication Not Provided
  Data: Port=0100 WWN=01:02:03:04:05:06:07:08
```

show.security.portBinding

Syntax

```
portBinding
```

Description

This command shows the port binding configuration for all ports.

Parameters

This command has no parameters.

Command example

```
Root> show security portBinding
```

Output

The port binding configuration data is displayed as a table that includes the following properties:

Port	The port number.
WWN Binding	The state of port binding for the specified port (active or inactive).
Bound WWN	The WWN of the device that is bound to the specified port. If this field is blank, no device is bound to the specified port.

Output example

The output from the *show.security.portBinding* command displays as follows:

```
Port     WWN Binding     Bound WWN
----     -----------     ----------------------
0        Active          AA:00:AA:00:AA:00:AA:00
1        Inactive        00:00:00:00:00:00:00:00
2        Inactive        CC:33:44:55:CC:33:44:55
3        Active          00:00:00:00:00:00:00:00
4        Inactive        00:00:00:00:00:00:00:00
5        Inactive        00:00:00:00:00:00:00:00
6        Inactive        00:00:00:00:00:00:00:00
7        Inactive        00:00:00:00:00:00:00:00
8        Inactive        00:00:00:00:00:00:00:00
9        Inactive        00:00:00:00:00:00:00:00
10       Inactive        00:00:00:00:00:00:00:00
11       Inactive        00:00:00:00:00:00:00:00
12       Inactive        00:00:00:00:00:00:00:00
13       Inactive        00:00:00:00:00:00:00:00
14       Inactive        00:00:00:00:00:00:00:00
15       Inactive        00:00:00:00:00:00:00:00
```

show.security.switchAcl

Syntax

```
switchAcl
```

Description

This command displays the contents of the Switch Access Control List.

Parameters

This command has no parameters.

Command example

```
Root> show security switchacl
Switch IP ACL State:    Disabled

Starting IP Address            Ending IP Address
---------------------- ----------------------
2001::222:192:11                2913:222::271
2001::1601:117                   2032::123
```

Output

The data is displayed as a table that includes the following properties:

Switch ACL State	The enabled state of the switch access control list.
Starting IP Address	The starting IP address of a range in the access control list.This IP address is in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format).
Ending IP Address	The ending IP address of a range in the access control list.This IP address is in either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format).

Output example

```
ACL State:  Disabled
Starting IP Address             Ending IP Address
-------------------             -----------------
110.80.1.1                      110.80.255.255
110.81.1.10                     110.81.1.255
200.11.15.1                     200.11.255.128
```

show.security.switchBinding

Syntax

```
switchBinding
```

Description

This command displays the switch binding configuration.

Parameters

This command has no parameters.

Command example

```
Root> show security switchBinding
```

Output

The switch binding configuration data is displayed as a table that includes the following properties:

Switch Binding State	The switch binding state, which can have the following values: *Disabled* *Enabled and Restricting F_Ports* *Enabled and Restricting E_Ports* *Enabled and Restricting All Ports*
Switch Binding Membership List	The WWNs of the members of the active SBML.

Output example

The output from the *show.security.switchBinding* command displays as follows:

```
Switch Binding State:   Enabled and Restricting E Ports
00:11:22:33:44:55:66:77
88:99:AA:BB:CC:DD:EE:FF
11:55:35:45:24:78:98:FA
```

show.snmp.accessTable

Syntax

```
accessTable [index]
```

Description

This command displays the configured values for the Access Table.

Parameters

This command has one optional parameter.

index	The index of the access entry. Valid values are 1 to 12.

Command example

```
Root> show snmp accessTable
```

Output example

The output from the *show.snmp.accessTable* command displays as follows:

```
SNMPv3 State:    Enabled
Index  Group Name
-----  ----------
1      group1
```

```
2
3
4       v1Group
5
6
7       v2Group
8
9
10      usmGroup
11      usmGroup
12
```

If the optional parameter, *index* is specified, the output from this command contains the following information:

SNMPv3 State	The status of SNMPv3 (Enabled or Disabled).
Index	The index of the access entry. Valid values are 1 to 6.
Group Name	The group name.
Security Model	The security model.
Security Level	The security level.
Read View	The read view name.
Write View	The write view name.
Notify View	The notify view name.

```
Config.SNMP> showAccessTable 1
Index:              1
Security Model:     Any
Security Level:     None
Group Name:         group1
Read View:          fcmgmt_3_1
Write View:         fceos
Notify View:        internet
```

NOTE
The command "config.snmp.showAccessTable" on page 119 has the functionality that is the same as this command.

show.snmp.targetTable

Syntax

```
targetTable [index]
```

Description

This command displays the configured values for the Target Table.

Parameters

This command has one optional parameter:

index	The index of the access entry. Valid values are 1 to 6.

Command example

```
Root> show snmp targetTable
SNMPv3 State:    Disabled

Index    Target IP               UDP Port   Community   MP Model
-----    --------------------  --------    ---------  --------
1         192::2341:231:451       172          xyz       SNMPv2
2         182::221                172                    SNMPv3
3
4
5
6
```

Output example

The output from the *show.snmp.targetTable* command displays as follows:

```
SNMPv3 State:    Enabled
Index  Target IP      UDP Port  Community                          MP Model
-----  -------------  --------  ---------------------------------  --------
1      172.19.16.169  162       public                             SNMPv1
2
3
4
5
6
```

If the optional parameter, *index*, is specified, the output from this command contains the following information:

SNMPv3 State	The status of SNMPv3 (Enabled or Disabled).
Index	The index number.
Target IP	The trap recipient IP (either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format)).
UDP Port	The UDP port for the trap recipient.
Community	The community name.
MP Model	The messaging model.
Security Name	The security name (username).
Security Model	The security model.
Security Level	The security level.

```
Config.SNMP> showTargetTable 1

Index:             1
Target IP:         172.19.16.169
UDP Port:          162
Community Name:    public
MP Model:          SNMPv1
Security Name:     user1
Security Model:    V1
Security Level:    No Authentication and No Privacy
```

show.snmp.userTable

Syntax

userTable

Description

This command displays the users configured presently in the USM Table.

Parameters

This command has no parameters.

Command example

Root> show snmp userTable

Output

This command displays the following switch configuration data:

SNMPv3 State	The status of SNMPv3 (Enabled or Disabled).
Index	The index number.
Username	The user name.
Auth Protocol	The Authentication Protocol.
Privacy Protocol	The Privacy Protocol.

Output example

The output from the *show.snmp.userTable* command displays as follows:

```
SNMPv3 State:    Enabled
Index  Username                         Auth Protocol      Privacy Protocol
-----  -------------------------------  -----------------  ----------------
1      User1                            No Authentication  No Privacy
2      User2                            HMAC-MD5           No Privacy
3      User3                            HMAC-SHA           DES
```

```
4
5
6
```

NOTE
This command and the command "config.snmp.showUserTable" on page 121 have the same functionality.

show.snmp.V3GroupTable

Syntax

```
V3GroupTable
```

Description

Displays the Security-to-Group table.

Parameters

This command has no parameters.

Command example

```
Root> show snmp v3GroupTable
```

Output

This command displays the following switch configuration data:

SNMPv3 State	The status of SNMPv3 (Enabled or Disabled).
Index	The index number.
Username	The user name.
Model	The security model.
Group Name	The group name.

Output example

The output from the *show.snmp.V3GroupTable* command displays as follows:

```
   SNMPv3 State:    Enabled
   Index  Username                          Model  Group Name
   -----  --------------------------------  -----  ----------
   1      User1                             V1     Group1
   2
   3
   4
   5
   6
```

show.snmp.viewTable

Syntax

viewTable

Description

This command displays the values for the VACM views that are presently configured.

Parameters

This command has no parameters.

Command example

```
Root> show snmp viewTable
```

Output

This command displays the following switch configuration data:

View Name	The name of the view.
Type	The type of the view.
Object ID	The object ID.

Output example

The output from the *show.snmp.viewTable* command displays as follows:

```
View Name                       Type               Object ID
------------------------------  -----------------  ---------
no_access                       View Excluded      .1.3.6.1
internet                        View Included      .1.3.6.1
management                      View Included      .1.3.6.1.2
experimental                    View Included      .1.3.6.1.3
private                         View Included      .1.3.6.1.4
snmpv3                          View Included      .1.3.6.1.6
fceos                           View Included      .1.3.6.1.4.1.289
fcmgmt_3_1                      View Included      .1.3.6.1.2.1.8888
fcmgmt_3_0                      View Included      .1.3.6.1.3.94
fcfe                            View Included      .1.3.6.1.3.42
system                          View Included      .1.3.6.1.2.1.1
ip                              View Included      .1.3.6.1.2.1.4
```

NOTE
The command "config.snmp.showViewTable" on page 123 has functionality that is the same as this command.

show.snmp.config

Syntax

```
config
```

Description

This command displays the switch SNMP configuration.

Parameters

This command has no parameters.

NOTE
The command "config.snmp.show" on page 118 has functionality that is identical to this command.

Command example

```
Root> show snmp config
```

Output

The switch configuration data is displayed as a table that includes the following properties:

SNMP Agent State	The state of the SNMP agent. If it is disabled, then the SNMP state does not respond to any requests, nor it produces any traps.
SNMPv3 State	The SNMPv3 state.
FA MIB Version Number	The version of the Fibre Alliance MIB (FA MIB) that the SNMP agent is configured to use.
Authentication Traps	The state of authentication traps to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the switch or director.
Index	The index in the community table.
Community. Name	The community name.
WriteAuth	The write authorization state of the community.
Trap Recipient	The protocol description of the trap recipient.
UDP Port	The UDP port number to which the switch or director sends traps for each recipient. This value is expressed in decimal and the default value is 162.

Output example

The output from the *show.snmp.config* command displays as follows:

```
SNMP Agent State:         Enabled
SNMPv3 State:             Disabled
FA MIB Version Number:    3.0
Authentication Traps:     Enabled
Index  Community Name                    WriteAuth  Trap Recipient   UDP Port
-----  --------------------------------  ---------  ---------------  --------
1      CommunityName1                    Enabled    123.123.123.123  162
2      CommunityName2                    Enabled    10.25.25.10      144
3      CommunityName3                    Disabled   132.44.85.224    162
4      public                            Enabled                     162
5
6
```

show.splzoning

Syntax

```
splzoning
```

Description

This command displays the special zones in the zone set.

Parameters

This command has no parameters.

Command example

```
Root>show splzoning
```

Output example

The output from the *show.splzoning* command displays as follows:

```
Example 1
Redirect_ZoneSet: eeeee
    Zone: red_0917_test
        Zone Member: 10:00:00:00:C9:3B:45:A0
        Zone Member: 10:00:00:00:C9:39:83:D3
        Zone Member: 10:00:00:00:C9:39:83:D4
        Zone Member: 10:00:00:00:C9:3B:45:A1

Example 2
    There are no rdzones
```

NOTE
This command shows splzoning status when the RD zone or special zone is already present. Example 2 displays when no RD zone is configured.

show.switch

Syntax

```
switch
```

Description

This command displays the switch attributes.

Parameters

This command has no parameters.

Command example

```
Root> show switch
```

Output

The switch attributes data is displayed as a table that includes the following properties:

State	The state of the switch (for example, online or offline).
R_A_TOV	The resource allocation timeout value (R_A_TOV) as set in the *config.switch.raTOV* command.
E_D_TOV	The error detect timeout value (E_D_TOV) as set in the *config.switch.edTOV* command.
Preferred Domain Id	The domain ID as set in the *config.switch.prefDomainId* command.
Switch Priority	The switch priority as set in the *config.switch.priority* command. For more information, see "config.switch.priority" on page 135.
Speed	The switch speed as set in the config.switch.speed command. (This command is only applicable for the Intrepid 6064 and So this information is only available in intrepid 6064..
Rerouting Delay	The rerouting delay as set in the *config.switch.rerouteDelay* command. For more information, see "config.switch.rerouteDelay" on page 136.
Interop Mode	The interoperability mode as set in the *config.switch.interopMode* command. For more information, see "config.switch.interopMode" on page 132.

Active Domain Id	The active domain ID of the switch or director. This ID may or may not be the same as the preferred domain ID.
World Wide Name	The WWN for the switch or director.
Insistent Domain Id	The configured insistent domain ID state as set in the *config.switch.insistDomainId* command. For more information, see "config.switch.insistDomainId" on page 132.
Domain RSCN	The configured domain RSCN state as set in the *config.switch.domainRSCN* command. For more information, see "config.switch.domainRSCN" on page 130.
Zoning RSCN	The configured Zoning RSCN state as set in the *config.switch.zoningRSCN* command. For more information, see "config.switch.webState" on page 141.
FC Address Domain Id	The domain ID of the switch derived from the Fibre Channel Address.
Limited Fabric RSCN	When enabled, fabric RSCNs are suppressed after an IPL.
Isolate Zone RSCN	When set to fabric filtering, fabric RSCNs are only sent to those members that need notification. When set to No Filtering, RSCNs are set to everyone when zoning information changes.
Safe Zoning	The safe zoning state.
ISL FSPF Cost	The method for computing the FSPF cost for ISLs.
Web Enable	The enabled state of web.
API Enable	The enabled state of API.
API Management IP	The IP address where the application that is managing the switch or director resides. If there is no application managing the switch, this will be the IP address of the switch.(either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format))
HA Mode	The enabled state of HA mode.
Domain ID Offset	The configured Domain ID offset of the switch
Password Exp. Time	The configured password expiration time for the management interface users of the switch.

Output example

The output from the *show.switch* command displays as follows:

```
Show> switch
State:                  Online
R_A_TOV:                20
E_D_TOV:                4
Preferred Domain Id:    1
Switch Priority:        Default
Speed:                  2 Gb/sec
```

```
Rerouting Delay:          Enabled
Interop Mode:             Open Fabric 1.0
Active Domain Id:         1
World Wide Name:          10:00:08:00:88:00:21:07
Insistent Domain Id:      Enabled
Domain RSCN:              Enabled
Zoning RSCN:              Disabled
FC Address Domain Id:     67 (hexadecimal)
Limited Fabric RSCN:      Disabled
Safe Zoning:              Enabled
ISL FSPF Cost:            By Port Speed
Web Enabled:              Enabled
API Enabled:              Enabled
HA Mode:                  Disalbed
API Management IP:        100.0.0.1
Domain ID offset:         96
Password Exp. Time:       365
```

show.system

Syntax

```
system
```

Description

This command displays a set of system attributes.

Parameters

This command has no parameters.

Command example

```
Root> show system
```

Output

The system attributes are displayed as a table that includes the following properties.

Name	The system name. For more information, see "config.system.name" on page 147.
Contact	The system contact as set in the *config.system.contact* command. For more information, see "config.syslog" on page 142.
Description	The system description. For more information, see "config.system.description" on page 146.
Location	The system description. For more information, see "config.system.location" on page 147.
Serial Number	The serial number for the system.

Type Number	The type number for the system.
Model Name	The model name for the system (for example, Sphereon 4500).
Model Number	The model number for the system. All products have the model number *001*, except 1 Gb sheet metal units, which are *002*.
EC Level	The engineering change level installed.
Firmware Version	The current firmware version installed.
Beaconing	The enabled state of unit beaconing (enabled or disabled) as set in the maint.system.beacon command.
Date/Time	The system date and time as set in the config.system.date command. For more information, see "config.system.date" on page 146.

Output example

The output from the *show.system* command displays as follows:

```
System Information
Name:             Joe's Switch
Description:      McDATA ED-6064 Fibre Channel Director
Contact:          Joe
Location:         Everywhere
Date/Time:        04/16/2001  10:34:01AM
Serial Number:    82420481
Type Number:      006064
Model Name:       ED-6064
Model Number:     001
EC Level:         1011231
Firmware Version: 04.01.00 Build 23
Beaconing:           Disabled
```

show.syslog

Syntax

```
syslog
```

Description

This command displays the syslog configuration.

Parameters

This command has no parameters.

Output

The syslog configuration is shown as a table of properties. The following properties are displayed:

Log	The index number of the server.
State	Whether syslog support is enabled.
Index	The index number of the server.
IP Address	The IP address of the server.(either V6 (hexadecimal colon based format) or V4 (4 bytes in dotted-decimal notation format))
Facility	The facility level for the server. Values are *Local 0 - Local 7.*

Command example

```
Root> show syslog
Syslog State:    Disabled

Index  IP Address             Facility
-----  -------------------    --------
1        2001::11               local0
2        2003::331:241:244      local1
3
```

show.thresholdAlerts.alerts

Syntax

```
alerts
```

Description

This command provides the name, type, and enabled state of each configured threshold alert, including both counter threshold alerts (CTAs) and throughput threshold alerts (TTAs).

Parameters

This command has no parameters.

Command example

```
Root> show thresholdAlerts alerts
```

Output

The threshold alert data displays as a table that includes the following properties:

Name	The name of the threshold alert, truncated to 45 characters.	
Type	The trigger statistic or threshold type of the alert (abbreviated to 17 characters). These include:	
	Tx Util	TTA - Transmit Utilization.
	Rx Util	TTA - Receive Utilization.
	Tx/Rx Util	TTA - Transmit or Receive Utilization.
	Link Resets Sent	CTA - Link Resets Sent.
	Link Resets Received	CTA - Link Resets Received.
	OLS Sent	CTA - OLS Sent.
	OLS Received	CTA - OLS Received.
	Link Failures	CTA - Link Failures.
	Sync Losses	CTA - Sync Losses.
	Signal Losses	CTA - Signal Losses.
	Protocol Errors	CTA - Primitive Sequence Errors/Protocol Errors.
	Invalid Tx Words	CTA - Invalid Tx Words.
	CRC Errors	CTA - CRC Errors.
	Discarded Frames	CTA - Discarded Frames.
	Frames Too Short	CTA - Frames Too Short.
	Delimiter Errors	CTA - Delimiter Errors.
	Address ID Errors	CTA - Address ID Errors.
	Cls2 BusiedFrms	CTA - Class 2 Busied Frames.
	Cls2 RejectedFrms	CTA - Class 2 Rejected Frames.
	Cls3 DiscardFrms	CTA - Class 3 Discarded Frames.
	Phys Lnk Err Set	CTA - Physical Link Errors Summed Set.
	Lnk Seq Cnt Set	CTA - Link Sequence Counts Summed Set.
	Logic Lnk Err Set	CTA - Logical Link Errors Summed Set.

	LIPS Detected	CTA - Loop Initialization Primitives detected (Sphereon 4300 and 4500 only).
	LIPS Generated	CTA - Loop Initialization Primitives Generated (Sphereon 4300 and 4500 only).
State	The enabled state of the CTA, either *enabled* or *disabled*.	

Output example

The output from the *show.thresholdAlerts.alert*s command displays as follows:

```
Name                                 Type                 State
-----------------------------------  -----------------    --------
Throughput Threshold #1              Rx Util              Enable
Threshold for CRC                    CRC Errors           Disabled
Safety #2                            Logic Lnk Err Set    Enabled
Safety #1                            Cls2 BusiedFrms      Disabled
```

show.thresholdAlerts.log

Syntax

```
log [clear]
```

Description

This command shows the contents of the threshold alert log. This log shows all the threshold alerts that have been triggered, including both counter threshold alerts (CTAs) and throughput threshold alerts (TTAs).

ATTENTION
If the switch is restarted (as occurs during IPL, IML, configuration reset, feature key installation, or firmware load) or is power cycled, the information in the threshold alert log is lost.

Parameters

This command has one parameter:

clear	Whether all threshold log entries should be cleared.

Command example

```
Root> show thresholdAlerts log
```

Output

The threshold alert log data displays as a table that includes the following properties:

Date/Time	The date and time of the alert.	
Name	The name of the threshold alert, truncated to 22 characters.	
Port	The type of threshold alert (CTAs only).	
Type	The trigger statistic or threshold type of the alert (abbreviated to 17 characters). These include:	
	Tx Util	TTA - Transmit Utilization.
	Rx Util	TTA - Receive Utilization.
	Tx/Rx Util	TTA - Transmit or Receive Utilization.
	Link Resets Sent	CTA - Link Resets Sent.
	Link Resets Received	CTA - Link Resets Received.
	OLS Sent	CTA - OLS Sent.
	OLS Received	CTA - OLS Received.
	Link Failures	CTA - Link Failures.
	Sync Losses	CTA - Sync Losses.
	Signal Losses	CTA - Signal Losses.
	Protocol Errors	CTA - Primitive Sequence Errors/Protocol Errors.
	Invalid Tx Words	CTA - Invalid Tx Words.
	CRC Errors	CTA - CRC Errors.
	Discarded Frames	CTA - Discarded Frames.
	Frames Too Short	CTA - Frames Too Short.
	Delimiter Errors	CTA - Delimiter Errors.
	Address ID Errors	CTA - Address ID Errors.
	Cls2 BusiedFrms	CTA - Class 2 Busied Frames.
	Cls2 RejectedFrms	CTA - Class 2 Rejected Frames.
	Cls3 DiscardFrms	CTA - Class 3 Discarded Frames.
	Phys Lnk Err Set	CTA - Physical Link Errors Summed Set.
	Lnk Seq Cnt Set	CTA - Link Sequence Counts Set.
	Logic Lnk Err Set	CTA - Logical Link Error Set.
	LIPS Detected	CTA - Loop Initialization Primitives Detected (Sphereon 4300 and 4500 only).

	LIPS Generated	CTA - Loop Initialization Primitives Generated (Sphereon 4300 and 4500 only).
Value	The increment or utilization value of the alert.	
Interval	The time interval of the alert.	

Output example

The output from the *show.thresholdAlerts.log* command displays as follows:

```
Date/Time         Name           Port   Type               Value  Int
----------------  -------------  -----  -----------------  -----  ---
05/26/02  10:58A  CTA Alert #4   2      Cls3 DiscardFrms   250    10
05/24/02  12:01A  CTA Alert #4   2      Cls3 DiscardFrms   250    10
05/22/02  10:58A  My test CTA    43     CRC Errors         35     30
05/20/02  08:01P  TTA Test #3    2      Tx Util            85    120
03/01/02  02:58A  CTA Alert #1   130    CRC Errors         100    60
```

show.zoning

Syntax

```
zoning
```

Description

This command shows the zoning configuration saved on the fabric.

Parameters

This command has no parameters.

Command example

```
Root> show zoning
```

Output

The zoning configuration data is displayed as a table that includes the following properties.

Active ZoneSet	The enabled status, name, and member zones of the zone set.

Output example

The output from the *show.zoning* command displays as follows:

```
Active Zone Set
Default Zone Enabled:  False
ZoneSet:  TheUltimateZoneSet
    Zone:  TheUltimateZone
           ZoneMember: Domain 10, Port 6
           ZoneMember: Domain 15, Port 2
           ZoneMember: Domain 2, Port 63
           ZoneMember: 10:00:00:00:C9:22:9B:64
           ZoneMember: 10:00:00:00:C9:22:9B:BD
    Zone:  TheNotSoUltimateZone
           ZoneMember: 10:00:00:00:C9:22:9B:AB
           ZoneMember: 10:00:00:00:C9:22:9B:C6
           ZoneMember: 10:00:00:00:C9:22:9B:AB
    Zone:  TheNotUltimateAtAllZone
           ZoneMember: Domain 2, Port 63
```

Appendix

Error Messages

A

This appendix lists and explains error messages for the Command Line Interface (CLI). Any error numbers that are not listed are reserved for future use.

The message that is returned is a string that includes the error number and the text of the message.

Message

Error 005: Busy

Description

The switch cannot process any requests at this time.

Action

Resubmit the request.

Message

Error 007: Not Authorized

Description

You are unable to get write authorization to save the configuration.

Action

Try again later.

Message

Error 008: Invalid Switch Name

Description

The value entered for the switch name is invalid.

Action

The name for the director or switch may contain 0–24 characters. Enter a name with 0–24 characters and resubmit. If spaces are used, enclose the name in quotation marks.

Message

Error 009: Invalid Switch Description

Description

The value entered for the switch Description is invalid.

Action

The description for the director or switch may contain 0–255 characters. Enter a description with 0–255 characters and resubmit. If spaces are used, enclose the description in quotation marks.

Message

Error 010: Invalid Switch Location

Description

The value entered for the switch location is invalid.

Action

The location for the director or switch may contain 0–255 characters. Enter a location with 0–255 characters and resubmit. If spaces are used, enclose the location in quotation marks.

Message

Error 011: Invalid Switch Contact

Description

The value entered for the switch contact is invalid.

Action

The contact for the director or switch may contain 0–255 characters. Enter a contact with 0–255 characters and resubmit. If spaces are used, enclose the contact in quotation marks.

Message

Error 012: Invalid Port Address

Description

The value entered for the port address is invalid.

Action

Enter a valid port address.

Message

Error 013: Invalid Port Number

Description

The value entered for the port number is invalid.

Action

Enter a port number within the range supported by your director or switch.

Message

Error 014: Invalid Port Name

Description

The value entered for the port name is invalid.

Action

The port name for the individual port may contain 0–24 characters. Enter a name with 0–24 characters and resubmit. If spaces are used, enclose the name in quotation marks.

Message

Error 015: Invalid BB Credit

Description

The value entered for the buffer-to-buffer credit is invalid.

Action

The buffer-to-buffer credit must be an integer in the range of 1–60. Enter a value in the correct range and resubmit.

Message

Error 016: Invalid R_A_TOV

Description

The value entered for the resource allocation time-out value is invalid.

Action

The R_A_TOV is entered in tenths of a second and must be entered as an integer in the range 10–1200 (1 second to 120 seconds). The R_A_TOV value must be larger than the E_D_TOV value. Check to be sure that all conditions are met and resubmit.

Message

Error 017: Invalid E_D_TOV

Description

The value entered for the error detection time-out value is invalid.

Action

The E_D_TOV is entered in tenths of a second and must be entered as an integer in the range 2–600 (0.2 second to 60 seconds). The E_D_TOV must be smaller than the R_A_TOV. Check to be sure that all conditions are met and resubmit.

Message

Error 018: Invalid TOV

Description

The E_D_TOV and R_A_TOV values are not compatible.

Action

Enter a valid E_D_TOV / R_A_TOV combination. The E_D_TOV must be smaller than the R_A_TOV.

Message

Error 020: Invalid Preferred Domain ID

Description

The value entered for the preferred domain ID for the director or switch is invalid.

Action

The preferred domain ID must be an integer in the range 1–31. Enter an appropriate value and resubmit.

Message

Error 021: Invalid Switch Priority

Description

The value entered for the switch priority is invalid.

Action

The switch priority entered for the director or switch must be one of the following: principal, neverprincipal, or default. Enter an appropriate value and resubmit. (Refer to the description of the command in "config.switch.priority" on page 135 for more information.)

Message

Error 029: Invalid Gateway Address

Description

The value entered for the gateway address is invalid.

Action

The new gateway address for the Ethernet interface must be entered in dotted decimal format (e.g. 0.0.0.0). Enter an appropriate gateway address and resubmit.

Message

Error 030: Invalid IP Address

Description

The value entered for the IP Address is invalid.

Action

The new IP address for the Ethernet interface must be entered in dotted decimal format (e.g. 10.0.0.0). Enter an appropriate IP address and resubmit.

Message

Error 031: Invalid Subnet Mask

Description

The value entered for the subnet mask is invalid.

Action

The new subnet mask for the Ethernet interface must be entered in dotted decimal format (e.g. 255.0.0.0). Enter an appropriate subnet mask and resubmit.

Message

Error 032: Invalid SNMP Community Name

Description

The value entered for the SNMP community name is invalid.

Action

The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and resubmit.

Message

Error 033: Invalid SNMP Trap Address

Description

The value entered for the SNMP trap address is invalid.

Action

The new SNMP trap address for the SNMP interface must be entered in dotted decimal format (e.g. 10.0.0.0). Enter an appropriate SNMP trap address and resubmit.

Message

Error 034: Duplicate Community Names Require Identical Write Authorization

Description

Two or more community names have been recognized as being identical, but their corresponding write authorizations are not identical.

Action

Enter unique SNMP community names or force write authorizations for duplicate community names to be identical and resubmit.

Message

Error 036: Port Already Swapped

Description

The port has already been swapped with another port and cannot be swapped again.

Action

Unswap the port before swapping it with another port.

Message

Error 037: Invalid Month

Description

The value of the month entered for the new system date is invalid.

Action

The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The month must contain an integer in the range 1–12. Enter an appropriate date and resubmit.

Message

Error 038: Invalid Day

Description

The value of the day entered for the new system date is invalid.

Action

The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The day must contain an integer in the range 1–31. Enter an appropriate date and resubmit.

Message

Error 039: Invalid Year

Description

The value of the year entered for the new system date is invalid.

Action

The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The year must contain an integer greater than 1980. Enter an appropriate date and resubmit.

Message

Error 040: Invalid Hour

Description

The value of the hour entered for the new system time is invalid.

Action

The format of the time parameter must be hh:mm:ss. The hour must contain an integer in the range 0–23. Enter an appropriate time and resubmit.

Message

Error 041: Invalid Minute

Description

The value of the minute entered for the new system time is invalid.

Action

The format of the time parameter must be hh:mm:ss. The minute must contain an integer in the range 0–59. Enter an appropriate time and resubmit.

Message

Error 042: Invalid Second

Description

The value of the second entered for the new system time is invalid.

Action

The format of the time parameter must be hh:mm:ss. The second must contain an integer in the range 0–59. Enter an appropriate time and resubmit.

Message

Error 044: Max SNMP Communities Defined

Description

A new SNMP community may not be defined without removing an existing community from the list.

Action

A total of 6 communities may be defined for SNMP. A new community can be added only after a current community is removed. Make the appropriate changes and resubmit.

Message

Error 045: Not Allowed While Switch Online

Description

The entered command requires that the director or switch be set offline.

Action

Set the switch offline and resubmit the command.

Message

Error 047: LIC install Active

Description

Cannot perform the specified action while a firmware download is in progress.

Action

Wait until the firmware download is complete and try again.

Message

Error 049: Invalid RADIUS Server UDP Port Number

Description

The RADIUS server UDP port number entered is invalid.

Action

Enter a valid UDP port. Valid values are 1 to 65535.

Message

Error 050: Invalid RADIUS Server Timeout Value

Description

The RADIUS server Timeout value entered is invalid.

Action

Enter a valid Timeout value. Valid values are 1 to 1000.

Message

Error 051: Invalid RADIUS Server Transmit Attempts Value

Description

The RADIUS server Retransmit value entered is invalid.

Action

Enter a valid Retransmit value. Valid values are 1 to 100.

Message

Error 052: Invalid RADIUS Server Deadtime Value

Description

The RADIUS server Deadtime entered is invalid.

Action

Enter a valid Deadtime value. Valid values are 0 to 1440.

Message

Error 053: Invalid RADIUS Key

Description

The RADIUS key entered is invalid.

Action

Enter a valid RADIUS key. Key length must be no more than 256 characters.

Message

Error 054: Buffer Limit Exceeded

Description

The total number of BB Credits configured cannot exceed the BB Credit buffer pool limit.

Action

Configure the total number of BB Credits for this switch to be less than or equal to the buffer pool limit.

Message

Error 055: Invalid Zone Name

Description

The value entered for the zone name is invalid.

Action

The zone name must be unique and contain 1–64 characters. The valid character set for the zone name can be found under “config.zoning.renameZoneSet” on page 161. Make the appropriate changes to the zone name and resubmit.

Message

Error 057: Duplicate Zone

Description

Two or more zone names in the zone set are identical.

Action

All zone names must be unique. Make the appropriate changes and resubmit.

Message

Error 059: Zone Name in Use

Description

Two or more zone names in the zone set are identical.

Action

All zone names must be unique. Make the appropriate changes and resubmit.

Message

Error 060: Invalid Number of Zone Members

Description

The entered command tried to add more zone members than the zone can hold.

Action

Reduce the number of zone members in the zone and resubmit the command.

Message

Error 061: Invalid Zone Member Type

Description

A zone member was entered that is neither a WWN nor a Domain, Port pair.

Action

Zone members must be expressed in WWN format or as a Domain, Port pair. Make the appropriate changes and resubmit. For more information, see "config.zoning.clearZone" on page 157 and "config.zoning.addPortMem" on page 154.

Message

Error 062: Invalid Zone Set Name

Description

The value entered for the zone set name is invalid.

Action

The zone set name must be contain 1–64 characters. The valid character set for the zone name can be found in "config.zoning.renameZoneSet" on page 161. Make the appropriate changes to the zone set name and resubmit.

Message

Error 064: Configuration changes have been limited to the API interface

Description

The API interface has restricted this interface from making configuration changes.

Action

To make configuration changes from this interface, the API interface must be updated to allow this interface to make changes.

Message

Error 065: Cannot remove the last CLI user with Administrator rights

Description

There has to be at least one CLI user with Administrator rights.

Action

To remove this user, add another CLI Administrator and then delete this user.

Message

Error 068: The Switch IP Access Control List is Full

Description

The list being activated has an invalid number of IP pairs.

Action

Make sure there is at least one IP address in the Access Control List.

Message

Error 069: Duplicate Port Name

Description

Two or more port names are identical.

Action

Port names must be unique. Make appropriate changes and resubmit. For more information, see "config.port.name" on page 52.

Message

Error 070: Invalid FRU Type

Description

The requested FRU does not exist on this product.

Action

Consult the installation/service manual for this product to find appropriate FRU names.

Message

Error 071: FRU Not Installed

Description

The requested FRU is not installed.

Action

Consult the installation/service manual for this product for appropriate action.

Message

Error 072: No Backup FRU

Description

The FRU swap cannot be performed because a backup FRU is not installed.

Action

Insert a backup FRU and resubmit the request or consult the installation/service manual for this product for appropriate action.

Message

Error 073: Port Not Installed

Description

The port specified is not installed on this product.

Action

Consult the installation/service manual on installing a port optic.

Message

Error 074: Invalid Number of Zones

Description

The specified zone set contains less than one zone or more than the maximum number of zones allowed for this product.

Action

A zone set must contain at least one zone to be considered valid. Add or remove zones accordingly to meet specified requirements.

Message

Error 075: Invalid Zone Set Size

Description

The zone set entered exceeds switch NVRAM limitations.

Action

Reduce the size of the zone set to meet specified requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.

Message

Error 076: Invalid Number of Unique Zone Members

Description

The zone entered contains more than the maximum number of zone members allowed per zone set for this product.

Action

Reduce the number of members in one or more zones and resubmit the command.

Message

Error 077: Not Allowed While Port Is Failed

Description

The port selected is in a failed or inactive state, or is in need of service.

Action

Consult the installation/service manual for appropriate action.

Message

Error 078: System Error Light On

Description

This unit is not able to beacon because the system error light is on.

Action

You must clear the system error light before unit beaconing may be enabled. Consult the installation/service manual for appropriate action.

Message

Error 079: FRU Failed

Description

The specified FRU has failed.

Action

Consult the installation/service manual for appropriate action.

Message

Error 081: Default Zone Enabled

Description

The request cannot be completed because the default zone is enabled.

Action

Disable the default zone and resubmit the command.

Message

Error 082: Invalid Interop Mode

Description

The value entered for the interoperability mode is not valid.

Action

The interoperability mode for the director or switch must be mcdata (McDATA Fabric 1.0) or open (Open Fabric 1.0). Make the appropriate changes and resubmit the command.

Message

Error 083: Not Allowed in Open Fabric Mode

Description

This request cannot be completed while this switch is operating in Open Fabric 1.0 mode.

Action

Configure the interop mode to McDATA Fabric 1.0 mode.

Message

Error 088: Invalid Feature Key Length

Description

The feature key installed is longer than the maximum length allowed.

Action

Be sure that the key has been entered correctly and resubmit. Contact your sales representative with any further problems.

Message

Error 090: Invalid Port Type

Description

The port type configured is invalid.

Action

A port may be configured to be an E_port, G_port, or F**_175: Invalid list index**port. Be sure the port is configured appropriately and resubmit the command.

Message

Error 091: E_Port Type Configured

Description

Ports are not allowed to be configured as E_Ports in S/390 mode.

Action

Configure the port as either a F_port or G_port and resubmit the command.

Message

Error 092: Not Allowed While Port Is Unblocked

Description

The port must be blocked to complete this request.

Action

Block the port and resubmit the command.

Message

Error 093: Not Allowed While FICON MS Is Installed

Description

This request cannot be completed because FICON Management Server is installed.

Action

This operation is not supported. No action necessary.

Message

Error 094: Invalid Feature Combination

Description

The features requested cannot be installed at the same time on one switch or director.

Action

Contact your sales representative.

Message

Error 099: Preferred Domain ID Cannot Be Zero

Description

This product cannot be configured to have a preferred domain ID equal to zero (0).

Action

Ensure that the ID is expressed as an integer in the range 1–31 and resubmit.

Message

Error 101: Command Not Supported on This Product

Description

This product does not support the requested command.

Action

Command not supported. No action necessary.

Message

Error 102: Switch Not Operational

Description

The request cannot be completed because the switch is not operational.

Action

Consult the installation/service manual and contact your service representative.

Message

Error 103: Port Diagnostic In Progress

Description

The request cannot be completed because a port diagnostic is running.

Action

Wait for the diagnostic to complete.

Message

Error 104: System Diagnostic In Progress

Description

The request cannot be completed because a system diagnostic is running.

Action

Wait for the diagnostic to complete.

Message

Error 105: Max Threshold Definitions Reached

Description

The maximum number of total threshold alerts has already been reached.

Action

Remove a threshold alert before adding the new threshold alert. A total of 16 counter and throughput threshold alerts is allowed.

Message

Error 106: Invalid Threshold Scope

Description

The scope of a threshold alert is not set to a valid state before you activate an alert.

Action

Set the scope of the threshold alert, then try to activate the alert.

Message

Error 107: Invalid Threshold State

Description

The scope of a threshold alert must be set before you activate an alert.

Action

Set the scope of the threshold alert, then try to activate the alert.

Message

Error 108: Invalid TTA Type

Description

The type of the throughput threshold alert has not been set.

Action

Set the type of the TTA, then try to activate the alert.

Message

Error 109: Invalid CTA Type

Description

The type of the counter threshold alert has not been set.

Action

Set the type of the CTA, then try to activate the alert.

Message

Error 110: Invalid Percent Utilization

Description

The type of the throughput threshold alert has not been set.

Action

Set the type of the TTA, then try to activate the alert.

Message

Error 111: Invalid Threshold Type

Description

The type of the threshold alert is not valid.

Action

Configure the type of the throughput threshold alert to one of the types found in the enumerated table for TTAs.

Message

Error 112: No Threshold Definition Given

Description

The threshold value for the alert was not configured before you attempted to activate the alert.

Action

Set the threshold value, then try to activate the alert.

Message

Error 115: Invalid Switch Speed

Description

The request cannot be completed because the switch is not capable of operating at the configured speed.

Action

Consult the installation/service manual to determine the speed capabilities of your product.

Message

Error 116: Switch Not Capable of 2 Gb/sec

Description

The request cannot be completed because the switch is not capable of operating at 2 Gbps.

Action

Consult the installation/service manual to determine the speed capabilities of your product.

Message

Error 117: Port Speeds Cannot be Set at Higher Data Rate than Switch Speed

Description

This request cannot be completed because the requested port speed is faster than the currently configured switch speed.

Action

The switch speed should first be configured to accommodate changes in the configured port speed. The ports cannot operate at a faster rate than the switch itself. Update the switch speed and resubmit the request. For more information, see "config.switch.speed" on page 138 and "config.port.show" on page 54.

Message

Error 118: Invalid Port Speed

Description

This request cannot be completed because the requested port speed is not recognized for this product.

Action

Port speeds may be set to 1 Gbps or 2 Gbps. Update the port speed and resubmit the request.

Message

Error 119: Switch Speed Not 2 Gb/sec

Description

This request cannot be completed because the switch speed has not been set to 2 Gbps.

Action

The switch speed must be set to 2 Gbps in order to accommodate a port speed of 2 Gbps. Update the switch speed and resubmit the request.

Message

Error 121: Invalid Credit Starvation Threshold

Description

An invalid credit starvation threshold has been entered.

Action

Submit the request with a valid value. The credit starvation threshold must be in the range 1-99.

Message

Error 122: Invalid Port Congestion Threshold

Description

An invalid port congestion threshold has been entered.

Action

Submit the request with a valid value. The port congestion threshold must be in the range 1-99.

Message

Error 134: Invalid Membership List

Description

Generic message to indicate a problem in either the switch binding or fabric binding membership list.

Action

Be sure that the membership list submitted does not isolate a switch already in the fabric. If this is not the case, you need to be aware of all fabric security rules and make sure that the list submitted adheres appropriately.

Message

Error 135: Invalid Number of Fabric Membership List Entries

Description

The number of fabric members submitted exceeds the maximum allowable entries of 31.

Action

The number of entries in the fabric membership list is limited to the total number of domain IDs available to the fabric. Make sure that the list (including the managed switch) contains no more than 31 entries.

Message

Error 136: Invalid Number of Switch Binding Membership List Entries

Description

The number of switch members submitted exceeds the maximum allowable entries of 256.

Action

The number of entries in the Switch Binding Membership List is limited to 256. Make sure that the list (including the managed switch) contains no more than 256 entries.

Message

Error 137: Invalid Fabric Binding State

Description

The fabric binding state submitted is not recognized by the CLI.

Action

The fabric binding state must be set to either “inactive” or “restrict.” See “config.security.fabricBinding” on page 80 for clarification of these states.

Message

Error 138: Invalid Switch Binding State

Description

The switch binding state submitted is not recognized by the CLI.

Action

The switch binding state must be set to one of the following: *disable*, *erestrict*, *frestrict*, or *allrestrict*. See “config.security.switchBinding” on page 96 for clarification of these states.

Message

Error 139: Insistent Domain ID's Must Be Enabled When Fabric Binding Active

Description

You attempted to disable insistent domain IDs while fabric binding was active.

Action

Insistent domain IDs must remain enabled while fabric binding is active. If fabric binding is set to inactive, the insistent domain ID state may be changed. It should be noted, however, that this can be disruptive to the fabric.

Message

Error 140: Invalid Insistent Domain ID State

Description

The request cannot be completed because an invalid insistent domain ID state has been submitted.

Action

The insistent domain ID state must be set to either *enable* or *disable*. For more information, see "config.switch.insistDomainId" on page 132.

Message

Error 141: Invalid Enterprise Fabric Mode

Description

The request cannot be completed because an invalid enterprise fabric mode has been submitted.

Action

The enterprise fabric mode must be set to either *activate* or *deactivate*. For more information, see "config.enterpriseFabMode.setState" on page 25.

Message

Error 142: Invalid Domain RSCN State

Description

The request cannot be completed because an invalid domain RSCN state has been submitted.

Action

The domain RSCN state must be set to either *enable* or *disable*. For more information, see "config.switch.domainRSCN" on page 130.

Message

Error 143: Domain RSCNs Must Be Enabled When Enterprise Fabric Mode Active

Description

You attempted to disable domain RSCNs while enterprise fabric mode was active.

Action

Domain RSCNs must remain enabled while the enterprise fabric mode is active. If enterprise fabric mode is set to inactive, the domain RSCN state may be changed. It should be noted, however, that this can be disruptive to the fabric.

Message

Error 144: The SANtegrity Feature Has Not Been Installed

Description

You attempted to activate a change to the fabric security configuration without first installing the SANtegrity feature key.

Action

If this key has not been installed, contact your sales representative.

Message

Error 146: Fabric Binding May Not Be Deactivated While Enterprise Fabric Mode Active

Description

You attempted to deactivate fabric binding while enterprise fabric mode was active.

Action

Fabric binding must be active while operating in enterprise fabric mode. The fabric binding state may be changed if enterprise fabric mode is deactivated. It should be noted, however, that this can be disruptive to the fabric.

Message

Error 148: Not Allowed While Switch Offline

Description

The switch must be online to complete this request.

Action

Change the state of the switch to ONLINE and resubmit the request.

Message

Error 149: Not Allowed While Enterprise Fabric Mode Enabled and Switch Active

Description

The request cannot be completed while the switch is online and enterprise fabric mode is active.

Action

This operation will be valid if the switch state is set to offline and enterprise fabric mode to inactive. It should be noted, however, that this can be disruptive to the fabric.

Message

Error 151: Invalid Open Systems Management Server State

Description

The request cannot be completed because the OSMS state submitted is invalid.

Action

The OSMS state may be set to either *enable* or *disable*. For more information, see "config.features.openSysMS" on page 28.

Message

Error 152: Invalid FICON Management Server State

Description

The request cannot be completed because the FICON MS state submitted is invalid.

Action

The FICON MS state may be set to either *enable* or *disable*. For more information, see "config.ficonMS.setMIHPTO" on page 40.

Message

Error 153: Feature Key Not Installed

Description

The request cannot be completed because the required feature key has not been installed to the firmware.

Action

Contact your sales representative.

Message

Error 154: Invalid Membership List WWN

Description

The request cannot be completed because the WWN does not exist in the switch binding membership list.

Action

Make sure that the WWN deleted matches the WWN in the Switch Binding Membership List. Make appropriate changes and resubmit the request.

Message

Error 155: Cannot Remove Active Member From List

Description

This member cannot be removed from the fabric security list because it is currently logged in.

Action

Fabric security rules prohibit any device or switch from being isolated from the fabric through a membership list change. If you truly intend to remove the device in question from the membership list, then there are several approaches to take. This request may be completed most nondisruptively by blocking the port (or physically removing the device from the managed switch) to which this device is attached and resubmitting the request.

Message

Error 156: Cannot Complete While Switch is Online and Fabric Binding Active

Description

The switch must be offline and Fabric Binding must be inactive before this feature can be disabled.

Action

Deactivating this feature can be disruptive to fabric operations. Take the switch offline and deactivate fabric binding before disabling this feature.

Message

Error 157: Access Control List is Disabled

Description

The switch must be offline and Fabric Binding must be inactive before this feature can be disabled.

Action

Deactivating this feature can be disruptive to fabric operations. Take the switch offline and deactivate fabric binding before disabling this feature.

Message

Error 158: Invalid Switch IP Access Control List IP Address Range

Description

The pair of IP addresses are invalid and cannot be added to the list.

Action

Make sure the IP addresses are valid and the first address is lower than the second.

Message

Error 159: Invalid IP Access Control List Pairs Count Value

Description

The list being activated has an invalid number of IP pairs.

Action

Make sure there is at least one IP address in the Access Control List.

Message

Error 161: The Switch IP Access Control List is Empty

Description

The management interface IP address is not in the list.

Action

The management IP must be in the list or the current connection would be lost.

Message

Error 162: List is full

Description

There is no more room for new entries in the list.

Action

Remove a different entry and try again.

Message

Error 163: FICON MS feature key must be installed

Description

The command is not available without the FICON MS feature key.

Action

Install the FICON MS feature key.

Message

Error 164: FICON CUP Zoning feature key must be uninstalled

Description

The operation cannot be completed with the FICON CUP Zoning key installed.

Action

Remove the FICON CUP Zoning feature key.

Message

Error 165: CUP Zoning feature key must be installed

Description

The command is not available without the FICON CUP Zoning feature key.

Action

Install the FICON CUP zoning feature key.

Message

Error 166: CUP Zoning feature must be enabled

Description

The command cannot be completed without the CUP Zoning feature enabled.

Action

Enable FICON CUP Zoning.

Message

Error 167: Diagnostics can not be run on inactive port

Description

The port is in the inactive state and diagnostics cannot be run.

Action

The port state must be changed out of the inactive state.

Message

Error 168: Duplicate member in the list

Description

The member is already in the list.

Action

Duplicate members are not allowed in the list.

Message

Error 169: Cannot enable CNT feature

Description

CNT support is in the wrong state.

Action

The enabled state for CNT support must be changed.

Message

Error 170: Duplicate IP Address range in the switch IP Access Control List

Description

Duplicate IP address pairs are not allowed in the Access Control List.

Action

This command is redundant, the member already exists in the list.

Message

Error 171: Invalid username

Description

The username is invalid.

Action

Enter a unique username using only the allowed characters and proper length.

Message

Error 172: Invalid list size

Description

The number of entries in the list is invalid.

Action

Make sure the list has at least one entry.

Message

Error 173: Invalid value

Description

The value being entered is invalid.

Action

Enter a valid value.

Message

Error 174: Invalid list data

Description

The list data is invalid.

Action

Correct the list to make it a valid list.

Message

Error 175: Invalid list index

Description

The index in the list is incorrect.

Action

Correct the index.

Message

Error 176: Entry not found in the list

Description

The desired entry in the list does not exist.

Action

Make sure the desired entry is in the list and it is being typed correctly.

Message

Error 177: Cannot remove the last Web user with Administrator rights

Description

At least one Administrator user must exist for each management interface.

Action

Add a new Administrator and then try again.

Message

Error 178: Invalid password

Description

The entered password is invalid.

Action

Enter a password using valid characters and a proper length.

Message

Error 179: Insistent Domain IDs must be enabled

Description

To complete this command, Insistent Domain IDs must be enabled.

Action

Enable Insistent Domain IDs.

Message

Error 180: Too many management interface users

Description

Only 25 management users can be added to the user database.

Action

Remove other management users to make room for a new one.

Message

Error 181: Preferred path must be disabled

Description

The Preferred Path feature must be disabled.

Action

Disable the Preferred Path feature.

Message

Error 182: Invalid fencing policy state

Description

The current fencing state is invalid.

Action

Enter a valid fencing state.

Message

Error 183: Invalid Enable Status

Description

The enable status is invalid.

Action

Enter a valid enable status.

Message

Error 184: Invalid Fencing Policy Time Period

Description

The entered period is invalid.

Action

Enter a valid period.

Message

Error 185: Invalid Limit Value for this Fencing Policy Type

Description

The entered limit is invalid.

Action

Enter a valid limit.

Message

Error 186: Cannot Block this Port

Description

Port is not blockable.

Action

Enter a valid port number.

Message

Error 187: Cannot Beacon this Port

Description

Cannot enable beaconing on this port.

Action

Enter a valid port number.

Message

Error 188: Port Swap Classification is not Identical

Description

Cannot swap ports because the port swap classification is not identical.

Action

Swap different ports or install a FRU with the same port classification.

Message

Error 189: Invalid Fencing Policy Type

Description

Invalid fencing policy type.

Action

Enter a valid fencing policy type.

Message

Error 190: Invalid Fencing Policy Port Type

Description

Invalid fencing policy port type.

Action

Enter a valid port or port type.

Message

Error 191: Max Fencing Policy Definitions Reached

Description

A new port fencing policy may not be defined without removing an existing port fencing policy from the list.

Action

A total of 14 policies may be defined for port fencing. A new policy can be added only after a current policy is removed. Make the appropriate changes and resubmit.

Message

Error 192: Invalid Fencing Policy Name

Description

Port fencing name is invalid.

Action

Configure a valid port fencing name.

Message

Error 193: Cannot Modify an Enabled Fencing Policy

Description

The policy cannot be modified while it is enabled.

Action

Disable the policy before modifying.

Message

Error 194: Cannot enable two policies of the same type that contain the same ports

Description

Two policies of the same type cannot be enabled if they have ports that are in both lists.

Action

Make sure the policy that is being enabled does not have the same port number as a policy that is enabled

Message

Error 195: Cannot enable two policies of the same type that contain same port scope

Description

Two policies of the same type cannot be enabled if they have the same port type.

Action

Make sure the policy that is being enabled does not have the same port type as a policy that is enabled.

Message

Error 196: Cannot enable two policies of the same type that contain default scope

Description

Two policies of the same type cannot be enabled if they are both using the default ports.

Action

Enable only one policy that is using the default ports.

Message

Error 197: Port list contains no ports

Description

The policy port list must contain ports or a port scope.

Action

Add ports or a port scope to the policy.

Message

Error 198: Duplicate Authentication Name

Description

Authentication names must be unique.

Action

Configure a unique authentication name.

Message

Error 201: Change Authorization Request Failed

Description

The switch did not accept the request to make a change to NVRAM.

Action

Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.

Message

Error 202: Invalid Change Authorization ID

Description

The switch will not accept a change request from this particular client.

Action

Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.

Message

Error 203: Another Client Has Change Authorization

Description

Another user is currently making changes to this switch.

Action

Be sure all parameters have been entered correctly and resubmit.

Message

Error 207: Change Request Failed

Description

The switch did not accept the request.

Action

Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.

Message

Error 208: Change Request Timed Out

Description

Authorization time to make NVRAM changes has expired.

Action

Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.

Message

Error 209: Change Request Aborted

Description

The switch did not accept the request.

Action

Be sure all parameters have been entered correctly and resubmit. Contact your service representative with further problems.

Message

Error 210: Busy Processing Another Request

Description

A different switch in the fabric was busy processing another request and could not complete the command.

Action

Be sure all parameters have been entered correctly and resubmit. Contact your service representative with continued problems.

Message

Error 211: Duplicate Zone

Description

Two or more zone names in the local zone set are identical.

Action

All zone names must be unique. Make the appropriate changes and resubmit.

Message

Error 212: Duplicate Zone Member

Description

A member was added that already exists in the zone.

Action

No action necessary.

Message

Error 213: Number of Zones Is Zero

Description

You are attempting to activate and empty zone set.

Action

The zone set must have at least one zone to be considered valid. Add a valid zone to the zone set and resubmit.

Message

Error 214: A Zone Contains Zero Members

Description

You are attempting to activate a zone set that contains at least one zone with zero members.

Action

Each zone in the zone set must contain at least one member. Add a valid member to the empty zone and resubmit.

Message

Error 215: Zone Set Size Exceeded

Description

The local work area zone set has outgrown the size limitations imposed by the Command Line Interface.

Action

Reduce the size of the zone set to meet CLI requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.

Message

Error 216: No Attached Nodes Exist

Description

There are no attached nodes.

Action

To add more members, attach more devices to the switch or add the members by WWN or Domain ID and port.

Message

Error 217: All Attached Nodes are in the Zone

Description

All the attached nodes are already in the zone.

Action

To add more members, attach more devices to the switch or add the members by WWN or Domain ID and port.

Message

Error 218: Invalid Port Number

Description

The value entered for the port number is invalid

Action

Enter a port number within the range supported by your director or switch.

Message

Error 219: Invalid Port Type

Description

The port type configured is invalid.

Action

A port may be configured to be an E_port, G_port, or F_port. Be sure the port is configured appropriately and resubmit the command. On the Sphereon 4300 and Sphereon 4500 only, FX_port and GX_port types are also supported. On the Sphereon 4300, the Fabric Capable feature must be installed to configure an E_Port, G_Port, or Gx_Port.

Message

Error 220: Cannot run diagnostics while a device is logged in to the port

Description

Diagnostics cannot be run while a device is logged into the port.

Action

Block the port to run diagnostics.

Message

Error 221: Cannot run diagnostics on an active E Port

Description

Diagnostics cannot be run on an active E_Port.

Action

Block the port to run diagnostics.

Message

Error 222: Invalid SNMP Community Index

Description

The value entered for the SNMP community index is invalid.

Action

The SNMP community index must be an integer in the range 1–6. Make the appropriate changes and resubmit the command.

Message

Error 223: Unknown Error

Description

The switch did not accept the request.

Action

Contact your service representative.

Message

Error 224: Invalid Argument

Description

One or more parameters are invalid for this command.

Action

Consult this manual (Chapter 2, CLI Commands) for appropriate parameter names. Parameters must be typed exactly to specification to be recognized correctly by the CLI.

Message

Error 226: Argument Is Too Long

Description

One or more parameters are invalid for this command.

Action

For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.

Message

Error 227: Invalid SNMP Community Name

Description

The value entered for the SNMP community name is invalid.

Action

The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and resubmit.

Message

Error 228: Invalid Write Authorization Argument

Description

The writeAuthorization parameter does not contain a valid value.

Action

Parameters must be typed exactly to specification to be recognized correctly by the CLI. For more information, see “config.security.ssl.setAPIState” on page 102.

Message

Error 229: Invalid UDP Port Number

Description

The udpPortNum parameter does not contain a valid value.

Action

Parameters must be typed exactly to specification to be recognized correctly by the CLI. For more information, see "config.switch.insistDomainId" on page 132.

Message

Error 230: Invalid WWN

Description

The WWN parameter does not contain a valid value.

Action

For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.

Message

Error 231: Invalid Port number

Description

The portNum parameter does not contain a valid value.

Action

For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.

Message

Error 232: Invalid Domain ID

Description

The domainID parameter does not contain a valid value.

Action

For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.

Message

Error 233: Invalid Member

Description

The zone member added is not valid.

Action

For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.

Message

Error 234: Invalid Command

Description

The CLI cannot associate an action with the submitted command. The command may be misspelled, required parameters may be missing, or the request may not be applicable to the branch of the CLI tree from which it was submitted.

Action

Consult the documentation for the command to be sure this command was entered correctly, all parameters are valid and present, and that the syntax is correct.

Message

Error 235: Unrecognized Command

Description

The CLI does not recognize the command and cannot perform the help '?' command as requested.

Action

The entered command is misspelled or the prompt is not positioned at the right place in the CLI command tree for this command. For the appropriate syntax, see the section of the manual that corresponds to the attempted command.

Message

Error 236: Ambiguous Command

Description

The CLI does not recognize the command issued.

Action

The CLI cannot interpret the command because a unique match cannot be identified. For the appropriate syntax, see the section of the manual that corresponds to the attempted command. Enter the complete command and resubmit.

Message

Error 237: Invalid Zoning Database

Description

There was an unidentifiable problem in the local zone set work area.

Action

Verify all parameters are entered correctly and resubmit. Otherwise, the pending zone set should be cleared and reconstructed.

Message

Error 238: Invalid Feature Key

Description

The feature key entered is invalid.

Action

Verify that the feature key was entered correctly and resubmit. Contact your service representative with further difficulties.

Message

Error 239: Fabric binding entry not found

Description

You requested to remove a fabric binding entry that is not in the pending fabric membership list.

Action

Verify that the correct entry (both WWN and Domain ID) is being requested for removal from the list and resubmit the request.

Message

Error 240: Duplicate fabric binding member

Description

You requested to add an entry to the fabric binding list that is already a member of the list.

Action

Verify that the correct entry (both WWN and Domain ID) is being requested for addition to the list and resubmit the request.

Message

Error 241: Comma-delimited mode must be active

Description

Comma-delimited mode must be active to execute this command

Action

Some commands require that comma-delimited mode be active (e.g. show.nameserverExt). Enable comma-delimited mode and re-issue the command.

Message

Error 244: Not allowed when Enterprise Fabric Mode is Active and Switch is Online

Description

This operation is not allowed while the switch is in Enterprise Fabric Mode and the switch is Online.

Action

Make sure Enterprise Fabric Mode is not enabled and the switch is offline.

Message

Error 245: Invalid increment value

Description

The increment value specified is not between 1 and 70560.

Action

Make sure the increment value given is between 1 and 70560.

Message

Error 246: Argument out-of-range/Duration is greater than Interval error

Description

The interval value specified is not between 5 and 70560 minutes.

Action

Make sure the increment value given is between 5 and 70560 minutes.

Message

Error 247: Invalid counter number

Description

The counter specified is not a valid number.

Action

Use the table output by the command "perf.thresholdAlerts.counter.showStatisticTable" on page 196 to find a valid counter value.

Message

Error 248: A counter must be assigned to this threshold alert

Description

A counter must be assigned to an alert before it is enabled.

Action

Use the command "perf.thresholdAlerts.counter.setCounter" on page 194 to set a counter before the alert is enabled.

Message

Error 249: At least one port or port type must be added to this threshold alert

Description

A port or port type must be assigned to an alert before it is enabled.

Action

Use the command "perf.thresholdAlerts.counter.addPort" on page 192 to add a port before the alert is enabled.

Message

Error 250: Invalid counter threshold alert name

Description

The name specified for the alert is not valid.

Action

Specify a counter threshold alert name that has already been created.

Message

Error 251: The threshold alert must be disabled

Description

The counter threshold alert to be modified or deleted is already enabled.

Action

Disable the threshold alert and then try the command again.

Message

Error 253: Cannot Remove a Member Currently Interacting with the Fabric

Description

Current members of the fabric must be included in the Fabric Binding List.

Action

Do not remove active fabric members from the pending Fabric Binding Membership List.

Message

Error 254: A utilization type must be assigned to this threshold alert

Description

A utilization type must be set before activating this threshold alert.

Action

Add a utilization type and then the threshold alert can be activated.

Message

Error 255: Invalid throughput threshold alert name

Description

The name of the threshold alert is incorrect.

Action

Either the name does not exist, or the new name cannot be used because it is illegal or a duplicate.

Message

Error 256: Invalid utilization type number

Description

The utilization type number does not exist.

Action

Select a valid utilization type number.

Message

Error 257: Invalid utilization percentage value

Description

The utilization percentage value is out of range.

Action

Select a valid utilization percentage value.

Message

Error 258: Invalid duration value

Description

The duration value in minutes is out of range.

Action

Select a valid duration value.

Message

Error 259: Invalid threshold alert name

Description

The name of the threshold alert is incorrect.

Action

The threshold alert name does not exist.

Message

Error 260: Not Allowed when SANtegrity feature is not installed on remote switch

Description

All switches in the fabric must have the SANtegrity feature key installed.

Action

Install the SANtegrity feature key on all switches in the fabric.

Message

Error 261: No Attached Members Exist

Description

There are no members attached to the switch.

Action

Check all connections and make sure attached devices are present.

Message

Error 262: All Attached Members are in the Membership List

Description

All attached fabric members are already in the membership list.

Action

The attempted action is redundant, all members are already in the list.

Message

Error 263: The SANtegrity Authentication feature key is not installed

Description

The SANtegrity Authentication feature key is not installed.

Action

Install the SANtegrity Authentication feature key.

Message

Error 264: The Preferred Path feature key is not installed

Description

The preferred path feature key must be installed.

Action

Install the preferred path feature key.

Message

Error 265: Duplicate threshold alert name

Description

The desired name for the threshold alert is already in use.

Action

Use a different name for the threshold alert.

Message

Error 266: Attached members cannot be added while fabric is building

Description

Attached members cannot be added while the fabric is building.

Action

The fabric is still building, wait a couple of seconds until it is complete.

Message

Error 268: RADIUS key too long

Description

The desired RADIUS key is too long.

Action

Use a shorter RADIUS key.

Message

Error 269: Invalid retransmit attempts. Must be between 1 and 100

Description

The desired retransmit attempt value is invalid.

Action

Select a retransmit value between 1 and 100.

Message

Error 270: Invalid timeout value. Must be between 1 and 1000

Description

The desired retransmit value is invalid.

Action

Select a timeout value between 1 and 10000.

Message

Error 271: Invalid deadtime value. Must be between 0 and 1440 minutes

Description

The desired deadtime value is invalid.

Action

Select a deadtime value between 0 and 1440.

Message

Error 272: Invalid IP address and port combination

Description

The desired host name and port combination does not exist in the database or it is invalid.

Action

Select a valid host name and port combination.

Message

Error 273: Passwords do not match

Description

The password does not match the confirm password.

Action

Re-enter the command and enter matching passwords.

Message

Error 274: Invalid interface combination

Description

The desired interface is not a valid interface.

Action

Select a valid interface value.

Message

Error 275: Invalid authentication role

Description

The desired role is not a valid role.

Action

Select a valid role. Valid roles are administrator and operator.

Message

Error 276: Invalid sequence authentication combination

Description

The desired sequence is not a valid sequence.

Action

Select a valid sequence. Valid sequences are RADIUS, local, and RADIUS local.

Message

Error 277: Roles cannot be assigned to a username with this interface

Description

The role of the selected username is not configurable.

Action

This operation is not supported. No action necessary.

Message

Error 278: CHAP authenticated passwords must be exactly 16 bytes

Description

The CHAP authentication password must be exactly 16 bytes.

Action

Enter a CHAP authentication password that is exactly 16 bytes.

Message

Error 280: Zone Member doesn't exist

Description

The desired zone member does not exist.

Action

Select a valid zone member.

Message

Error 281: Zone doesn't exist

Description

The desired zone does not exist.

Action

Select a valid zone name.

Message

Error 282: Conflicting Domain ID for the specified WWN

Description

The desired Domain ID is already in use.

Action

Select a different Domain ID.

Message

Error 283: Conflicting WWN for the specified Domain ID

Description

The WWN is already in use.

Action

Select a different WWN.

Message

Error 284: FICON CUP Zoning host control list is full

Description

A new host may not be entered without removing an existing host from the list.

Action

A total of 8 hosts may be defined for the FICON CUP Zoning host control list. A new host can be added only after a current host is removed. Make the appropriate changes and resubmit.

Message

Error 285: WWN not found in host control list

Description

The desired WWN is not in the host control list.

Action

Select a WWN that is in the host control list.

Message

Error 286: Invalid number of NPIV allowed logins

Description

The desired value for NPIV allowed logins is invalid.

Action

Select a value between 1 and 256.

Message

Error 287: Port is unaddressable

Description

The desired port cannot be configured because it is unadressable.

Action

This operation is not supported. No action necessary.

Message

Error 288: The NPIV feature key must be installed

Description

The NPIV feature key must be installed to complete this operation.

Action

Install the NPIV feature key.

Message

Error 289: Duplicate policy name

Description

A policy cannot be added if it has the same name as an existing policy.

Action

Select a different policy name.

Message

Error 290: No Optic Installed

Description

There is not an optic in the port for the specified port number.

Action

Select a different port number, or plug in an optic.

Message

Error 291: Port Inaccessible

Description

The port is inaccessible for the given port number.

Action

Select a different port number.

Message

Error 292: Port Number out of Range

Description

The specified port number is out of range for the given switch/director.

Action

Select a different port number.

Message

Error 294: Invalid RADIUS Index

Description

The specified RADIUS index is invalid.

Action

Enter a valid RADIUS index. Valid indexes are 1 to 3.

Message

Error 295: Invalid MIHPTO value

Description

The MIHPTO value is invalid.

Action

Enter a valid MIHPTO value.

Message

Error 296: Cannot delete last EPort user with current authentication setting

Description

You cannot remove the last E_Port user with the current authentication settings.

Action

Modify the E_Port authentication settings.

Message

Error 297: Cannot delete last N_Port user with current setting authentication setting

Description

You cannot remove the last N_Port user with the current authentication settings.

Action

Modify the N_port authentication settings.

Message

Error 298: Cannot delete last API user with current authentication setting

Description

You cannot remove the last API user with the current authentication settings.

Action

Modify the API authentication settings.

Message

Error 299: Chap secret not defined

Description

The CHAP secret must be defined (for Open Systems Management Server before enabling Outgoing Authentication.)

Action

Define a CHAP Secret (for Open Systems Management Server).

Message

Error 300: No user defined for this Interface

Description

You cannot perform the specified action unless a user is defined for the interface.

Action

Create a user for the interface.

Message

Error 301: RADIUS server undefined

Description

You cannot perform the operation until a RADIUS server is configured. (You cannot enable RADIUS Authentication if there is no RADIUS server configured.)

Action

Configure a RADIUS server (before enabling RADIUS Authentication).

Message

Error 302: Pending Default Zone Member Count Exceeds Threshold

Description

You cannot enable default zoning if there are more than 64 devices not being zoned.

Action

Bring the number of unzoned devices down to 64.

Message

Error 303: Destination Domain ID cannot be same as source Domain ID

Description

The preferred path entered is invalid. (One reason the preferred path could be invalid is if the destination domain ID is the same as the local switch ID.)

Action

Enter a valid preferred path.

Message

Error 304: Radius Authentication Present. Cannot remove all Radius Servers

Description

You cannot remove all the RADIUS Server configurations if RADIUS Authentication is enabled on any interface.

Action

Disable RADIUS Authentication on all interfaces and then remove the last RADIUS server configuration.

Message

Error 305: Operating mode is not OSMS

Description

You cannot enable CT Outgoing Authentication when Open Systems Management Server is disabled.

Action

Enable Open Systems Management Server before enabling CT Outgoing Authentication.

Message

Error 306: CT Outgoing Authentication is enabled

Description

You cannot disable Open Systems Management Server when CT Outgoing Authentication is enabled.

Action

Disable CT Outgoing Authentication before disabling Open Systems Management Server.

Message

Error 307: The preferred path does not exist

Description

You tried to clear a path that does not exist.

Action

None

Message

Error 308: Invalid line speed combination

Description

The Ethernet speed/duplex combination is invalid.

Action

Enter a valid Ethernet speed/duplex combination.

Message

Error 310: FICON Management Server must be enabled

Description

You cannot perform this operation until the FICON Management Server is enabled.

Action

Enable the FICON Management Server.

Message

Error 311: FICON CUP Zoning must be disabled

Description

You cannot perform this operation until the FICON Management Server is disabled.

Action

Disable the FICON Management Server.

Message

Error 321: Invalid syslog facility number

Description

The syslog facility number is invalid

Action

Select a valid syslog facility number.

Message

Error 323: Invalid trigger start offset

Description

The trigger start offset value is invalid.

Action

Select a valid trigger start offset value.

Message

Error 324: Invalid trigger start bit pattern

Description

The trigger start bit pattern is invalid.

Action

Select a valid trigger start bit pattern.

Message

Error 325: Invalid trigger end offset

Description

The trigger end offset value is invalid.

Action

Select a valid trigger end offset value.

Message

Error 326: Invalid trigger end bit pattern

Description

The trigger end bit pattern is invalid.

Action

Select a valid trigger end bit pattern.

Message

Error 327: Invalid trigger

Description

The trigger is invalid.

Action

Enter a valid trigger value.

Message

Error 328: Invalid syslog index

Description

The syslog index is invalid.

Action

Select a valid syslog index.

Message

Error 330: Invalid trace route source

Description

The trace route source value is invalid.

Action

Select a valid WWN or Port ID for the trace route source.

Message

Error 331: Invalid trace route destination

Description

The trace route destination value is invalid.

Action

Select a valid WWN or Port ID for the trace route destination.

Message

Error 332: Unable to run a trace route at this time

Description

The trace route is unable to run.

Action

Wait a little while and run the trace route again.

Message

Error 333: Invalid Port ID

Description

The Port ID is invalid.

Action

Enter a valid Port ID.

Message

Error 336: Invalid SSL renegotiation megabyte value

Description

The SSL renegotiation megabyte value is invalid.

Action

Enter a valid SSL renegotiation megabyte value.

Message

Error 337: Invalid SNMP table index

Description

The SNMP table index is invalid.

Action

Select a valid index.

Message

Error 339: Invalid SNMPv3 user table index

Description

The user table index is invalid.

Action

Enter a valid index.

Message

Error 340: Invalid SNMPv3 username

Description

The username is invalid.

Action

Select a valid username.

Message

Error 341: Invalid SNMPv3 authentication protocol

Description

The authentication protocol is invalid.

Action

Select a valid authentication protocol.

Message

Error 342: Invalid SNMPv3 authentication key

Description

The authentication key is invalid.

Action

Select a valid authentication key.

Message

Error 343: Invalid SNMPv3 privacy protocol

Description

The privacy protocol is invalid.

Action

Select a valid privacy protocol.

Message

Error 344: Invalid SNMPv3 privacy key

Description

The privacy key is invalid.

Action

Select a valid privacy key.

Message

Error 345: Invalid SNMPv3 target table index

Description

The target table index is invalid.

Action

Select a valid index.

Message

Error 346: Invalid SNMPv3 target IP

Description

The Target IP Address is invalid.

Action

Enter a valid IP Address.

Message

Error 347: Invalid SNMPv3 UDP port number

Description

The UDP Port number is invalid.

Action

Select a valid UDP port number.

Message

Error 348: Invalid SNMPv3 community name

Description

The community name is invalid.

Action

Enter a valid community name.

Message

Error 349: Invalid SNMPv3 MP model

Description

The MP model is invalid.

Action

Enter a valid MP model.

Message

Error 350: Invalid SNMPv3 security name

Description

The security name is invalid.

Action

Enter a valid security name.

Message

Error 351: Invalid SNMPv3 group name

Description

The group name is invalid.

Action

Enter a valid group name.

Message

Error 352: Invalid SNMPv3 security model

Description

The security model is invalid.

Action

Enter a valid security model.

Message

Error 353: Invalid SNMPv3 security level

Description

The security level is invalid.

Action

Enter a valid security level.

Message

Error 354: Invalid SNMPv3 access table index

Description

The access table index is invalid.

Action

Enter a valid index.

Message

Error 360: The number of days for key generation is out of range.

Description

The number of days for the key generation is invalid.

Action

Enter a valid number of days for key generation.

Message

Error 361: An internal error occurred when generating the key.

Description

An error occurred while generating the SSL key.

Action

None

Message

Error 362: Duplicate SNMPv3 user name

Description

You can't have two SNMPv3 usernames that are the same.

Action

Enter a different value for the username.

Message

Error 363: Invalid SNMPv3 group table index

Description

The group table index is invalid.

Action

Enter a valid index.

Message

Error 364: SNMPv3 duplicate configuration

Description

The group name, security name, security model combination must be unique.

Action

Enter a valid group name, security name, and security model combination.

Message

Error 367: Invalid SNMPv3 access group name

Description

The access group name is invalid.

Action

Enter a valid access group name.

Message

Error 371: Unable to set HA mode

Description

The HA mode cannot be set.

Action

Contact your service representative.

Message

Error 372: The IP ACL pair does not exist in the Switch Access Control List

Description

The IP ACL pair is not in the list.

Action

None

Message

Error 373: Configuration not allowed while SNMPv3 is enabled

Description

You cannot perform the desired operation while SNMPv3 is enabled.

Action

Disable SNMPv3 before continuing.

Message

Error 374: Invalid SNMPv3 securitytogroup index

Description

The security to group table index is invalid.

Action

Enter a valid index.

Message

Error 376: The Local Switch WWN or DID conflicts with another member

Description

There is a member in the FBML that has the same WWN or domain ID as the local switch.

Action

Remove the conflicting entry and then add the local switch to the list.

Message

Error 377: HA Mode cannot be turned off with both Power Supply connected

Description

When both power supplies are connected, the HA Mode cannot be disabled.

Action

None

Message

Error 378: Duplicate IP address setting

Description

The IP address already exists.

Action

Choose a different IP Address or remove the existing entry.

Message

Error 379: Changing of QPM port mode can only start with an even numbered port

Description

Only even numbered ports can be configured.

Action

Specify the complementary port of the port that is specified to configure the mode of the port.

Message

Error 380: Invalid Domain ID offset

Description

The offset value specified is invalid.

Action

Specify a different domain ID offset value.

Message

Error 381: Invalid PORT Mode specified

Description

The mode of operation specified is invalid.

Action

Specify the mode of operation of the port as Burst or Sustained.

Message

Error 382: Blade is not a QPM

Description

The port that is being configured is not a QPM.

Action

The mode of operation of a port can be configured only for ports on a QPM.

Message

Error 383: Invalid Password Expiry Limit

Description

The password expiration time specified is invalid.

Action

The password expiration time should be in the range 0-3650.

Message

Error 384: Count specified to ping a destination is invalid

Description

The ping count specified is invalid.

Action

The count can have a value from 1 to 10.

Message

Error 385: Timeout value specified for ping is invalid

Description

The ping response timeout specified is invalid.

Action

The timeout can have a value from 1 to 10.

Message

Error 386: Unable to complete ping request at this time

Description

Ping could not be completed.

Action

None.

Message

Error 387: Snapshot Database not Available

Description

The snapshot database was not saved previously.

Action

Issue the saveSnapshot command and then re-issue the command.

Message

Error 388: Could not save Name Server snapshot

Description

The snapshot of the Name Server database could not be saved.

Action

Issue the saveSnapshot command again.

Message

Error 389: There is no Name Server snapshot saved

Description

The snapshot of the Name Server database was not saved.

Action

Use the saveSnapshot command and then re-issue this command.

Message

Error 390: Invalid Login Banner Line Index

Description

The line number specified for the banner text is invalid.

Action

The line number can have a value between 0-24.

Message

Error 391: Invalid destination domain specified

Description

The destination domain ID specified is invalid.

Action

The domain Id can have a value between 1-31.

Message

Error 392: Invalid Source Port specified

Description

The port number specified is invalid.

Action

Specify a valid port number.

Message

Error 393: Invalid SSH renegotiation megabyte value

Description

The renegotiation megabyte value that was specified is invalid.

Action

The renegotiation value can have a value between 1-1000.

Message

Error 394: Password must be different from last 3 passwords

Description

The new password is the same as one of the previous three passwords.

Action

Specify the new password to be different from the previous three passwords.

Message

Error 395: Port Address Is Out Of Range

Description

The port address specified is invalid.

Action

Specify a valid port address when issuing the command.

Message

Error 396: logical error

Description

An internal logical error has occurred.

Action

None.

Message

Error 397: Unable to respond to the request

Description

The destination was not able to respond to the ping request.

Action

None.

Message

Error 398: Resource unavailable

Description

A resource that was needed for completing this request was not available.

Action

None.

Message

Error 399: Source not in fabric

Description

The specified port is not in the fabric.

Action

Specify a valid port.

Message

Error 400: Command to remote switch timed out

Description

Did not get a response within the specified timeout.

Action

None.

Message

Error 401: Port no longer online

Description

The specified port is not online.

Action

None.

Message

Error 402: Proxy transaction aborted

Description

The operation was aborted.

Action

None.

Message

Error 402: Proxy received, but invalid response

Description

A response was received, but it was an invalid response.

Action

None.

Message

Error 402: Proxy transaction aborted

Description

The operation was aborted.

Action

None.

Message

Error 404: Good response, but invalid payload

Description

A response was received; however the response contained an invalid response.

Action

None.

Message

Error 405: Logical error in proxy response

Description

An error occurred in the ping response.

Action

None.

Message

Error 406: Destination not logged in

Description

The destination specified was not online.

Action

Make the destination switch online and then re-issue the ping request.

Message

Error 407: No path to the destination from the source

Description

There is no path from the specified source to the destination

Action

None

Message

Error 408: Invalid CIDR log event specified

Description

The log setting specified is invalid.

Action

Specify a valid log setting.

Message

Error 409: An association already exists

Description

An association already exists.

Action

Specify a different association – nickname and WWN combination.

Message

Error 410: Could not find the existing association

Description

The specified association is not in the pending association list.

Action

Specify a different association.

Message

Error 411: The pending associations could not be saved

Description

The save operation for Nickname associations failed.

Action

None.

Message

Error 411: Invalid alias

Description

An invalid alias was specified.

Action

Assign a valid alias for the WWN.

Message

Error 414: No aliases associations available

Description

The association list is empty.

Action

None.

Message

Error 415: The active associations could not be loaded

Description

The active association list could not be copied to the pending association list.

Action

None.

Message

Error 416: The Association list has not been updated with the active associations

Description

The active associations were updated by an external source.

Action

Use the replacePending command and re-issue all the changes.

Message

Error 417: Invalid WWN or alias specified

Description

The specified WWN or alias was not found in the active association list.

Action

None.

Message

Error 418: Maximum Associations count has been reached

Description

Only 250 associations are possible and the limit has been reached.

Action

None.

Message

Error 419: The Associations have been modified externally

Description

The associations have been modified in a different switch in the fabric and have been synchronized fabric-wide and hence the checksum has changed.

Action

Update the pending list and re-issue the commands.

Message

Error 420: Unable to handle request at this time

Description

An internal error occurred.

Action

None.

Message

Error 421: Nickname cannot be a WWN

Description

An alias cannot be a WWN.

Action

Assign a different alias to the WWN.

Message

Error 422: Invalid FCID

Description

The FCID specified is invalid.

Action

Specify a valid FCID.

Message

Error 423: Duplicate Radius server entry

Description

The specified Radius already exists in the configured list of servers.

Action

Specify a new valid server.

Message

Error 424: Unable to set default zone state

Description

The operation to set the default zone state failed.

Action

None.

Message

Error 425: Invalid login banner length

Description

The login banner line length is too long.

Action

Enter a login banner line of 80 characters or less.

Message

Error 426: Invalid ping destination

Description

An invalid FCID was entered.

Action

Specify a valid FCID.

Message

Error 427: Invalid snmp udp port number.

Description

The SNMP UDP port number is not correct.

Action

Specify the valid SNMP UDP port.

Message

Error 428: Invalid Login Banner text.

Description

The text of the login banner is invalid.

Action

Specify a valid text for the login banner.

Message

Error 429: Invalid POM log event specified.

Description

The event specified is invalid.

Action

Specify a valid event for POM Report logging.

Message

Error 430: Invalid Port Type and Speed combination

Description

"Negotiate Burst 4 Max" and "4 Burst" can be set with F_ports only.

Action

For the QPM card, change the port type to F_port for speed setting of "Negotiate Burst 4 Max" and "4 Burst".

Message

Error 431: Ping to well-known address is disallowed

Description

A well-known FCID is entered.

Action

Specify a valid FCID other than the well-known address.

Message

Error 432: Not allowed while fabric not operational

Description

The operation is not allowed while fabric is not operational.

Action

Try again after fabric becomes operational.

Message

Error 434: Not allowed while the port is online

Description

Not allowed while the port is online

Action

Block the port before changing BB credit

Message

Error 435: INVALID_IPV6_GATEWAY_ADDRESS

Description

when a keyin value is invalid.

Action

Give proper ipv6 gateway address

Message

Error 436: INVALID_IPV6_ADDRESS

Description

This error message appears when you keyin an invalid IPV6 address

Action

Give proper ipv6 address

Message

Error 437: INVALID_IPV6_PREFIX

Description

The range of prefix mask is invalid.

Action

Give prefix mask in range 4 to 128

Message

Error 438: IPV6_DISABLED

Description

The state of switch in IPV6 is disabled.

Action

Enable the ipv6 state

Message

Error 439: IPV6_RESERVED

Description

This IP is reserved by IETF, try another IPv6 address.

Action

Give an ipv6 address which does not exist in the IETF list

Message

Error 440: TUNNEL_DISABLED

Description

The tunneling support is not enabled

Action

Enable the tunneling support

Message

Error 441: TRIAL_KEY_EXPIRED

Description

Trial key expired and can no longer be used

Action

The trial key installed cannot be used until switch NVRAM memory is cleared.

Message

Error 442: Not allowed, SBML is exceeding its maximum limit.

Description

Switch Binding membership list is full. So, new members are not allowed.

Action

SBML should have enough space to accommodate new members.

Message

443: Invalid Slowdrainer logging event

Description

Slow drainer log event is invalid

Action

None

Message

444: Not allowed while switch is in fabric

Description

Deleting Redirect Zone is not allowed while switch is in fabric.

Action

Try to delete the Redirect zone from B-model switch or bring the switch as standalone.

Message

445: Entry already exists for the specified index

Description

There is already an entry for the specified index

Action

None

Message

446: Ipacl is Enabled with only ipV6 Entries

Description

There is no IPv4 addresses in the ACL list i.e., purely IPv6 addresses. Enabling IPv6 support at this time causes loss of access to the switch, since you are currently logged in with IPv4 address.

Action

Add your v4 address in the list and try enabling IPv6.

Message

Error 447: INVALID_TUNNEL_ROUTE

Description

Invalid tunnel route

Action

Default gateway cannot be assigned as tunnel route.

Message

Error 448: Zone set contains members that are not allowed in open mode

Description

Some of the members in the Zone set are in port-domain format which is not allowed in open mode.

Action

Members in the zone set should not be in port-domain format in open mode.

Appendix

Commands and Corresponding Releases

B

Table 8, shows the commands that are valid in the Enterprise Operating System (M-EOS) Command Line Interface (CLI) and the release in which the command was added to the CLI. The commands are organized by release, and are in alphabetical order within the release.

TABLE 8 Commands and Releases

E/OS Releases	Command
9.9.2	*show.fabric.agshow*
9.9.2	*show.fabric.agshow local*
9.9.2	*show.fabric.agshow remote*
9.9.2	*show.fabric.dcfmtable*
9.9	*config switch blockDupWWN*
9.8	*config.tunnel.edit*
9.8	*config.tunnelroute.edit*
9.8	*config.zoning.showSplZoneState*
9.8	*config.zoning.showActiveSpl*
9.8	*config.zoning.disableSplZoneSet*
9.8	*perf.slowdrainer.sdreport*
9.8	*perf.slowdrainer.show*
9.8	*show.splzoning*
9.7	*config.ip.v6*
9.7	*config.switch.setipv6*
9.7	*config.tunnel.add*
9.7	*config.tunnel.delete*
9.7	*config.tunnel.show*
9.7	*config.tunnelroute.add*
9.7	*config.tunnelroute.delete*
9.7	*config.tunnelroute.show*
9.7	*config NPIV setALPAREstate*
9.1	*config.alias*
9.1	*config.alias.activatePending*
9.1	*config.alias.add*
9.1	*config.alias.clearPending*
9.1	*config.alias.delete*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
9.1	*config.alias.replacePending*
9.1	*config.alias.setCLIState*
9.1	*config.alias.setWebState*
9.1	*config.alias.showActive*
9.1	*config.alias.showPending*
9.1	*show.activeAlias*
9.1	*show.openSysMS.platformInfo*
9.0	*config.NSTools*
9.0	*config.NSTools.clearSnapshot*
9.0	*config.NSTools.saveSnapshot*
9.0	*config.NSTools.showSnapDiff*
9.0	*config.NSTools.showSnapshot*
9.0	*config.security.authentication.user.passExpTime*
9.0	*config.security.ssh.setRenegotiationMB*
9.0	*config.snmp.sendTestTrap*
9.0	*config.switch.banner*
9.0	*config.switch.banner.bannerText*
9.0	*config.switch.banner.setCLIState*
9.0	*config.switch.banner.setWebState*
9.0	*config.switch.banner.show*
9.0	*config.switch.domainIDOffset*
9.0	*perf.AFD*
9.0	*perf.AFD.HDDReport*
9.0	*perf.AFD.POMReport*
9.0	*perf.AFD.show*
9.0	*show.epFrameLog.removeFilterPort*
9.0	*show.fabric.ping*
9.0	*show.fabric.showRouteTable*
9.0	*show.nameServerFC4Types*
8.0	*config.security.ssl.generateKeys*
8.0	*config.security.ssl.resetKeys*
8.0	*config.security.ssl.setAPIState*
8.0	*config.security.ssl.setRenegotiationMB*
8.0	*config.security.ssl.setWebState*
8.0	*config.security.ssl.show*
8.0	*config.snmp.addAccessEntry*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
8.0	*config.snmp.deleteAccessEntry*
8.0	*config.snmp.addTargetParams*
8.0	*config.snmp.addUserEntry*
8.0	*config.snmp.addV1Target*
8.0	*config.snmp.addV2Target*
8.0	*config.snmp.addV3Group*
8.0	*config.snmp.addV3Target*
8.0	*config.snmp.deleteAccessEntry*
8.0	*config.snmp.setSNMPv3State*
8.0	*config.snmp.deleteUserEntry*
8.0	*config.snmp.deleteV3Group*
8.0	*config.snmp.setSNMPv3State*
8.0	*config.snmp.showAccessTable*
8.0	*config.snmp.showTargetTable*
8.0	*config.snmp.showUserTable*
8.0	*config.snmp.showV3GroupTable*
8.0	*config.snmp.showViewTable*
8.0	*config.snmp.validateUser*
8.0	*config.switch.apiState*
8.0	*config.switch.haMode*
8.0	*config.switch.webState*
8.0	*config.switch.apiState*
8.0	*config.switch.safeZoning*
8.0	*config.switch.islFSPFCost*
8.0	*config.syslog*
8.0	*config.syslog.addServer*
8.0	*config.syslog.deleteServer*
8.0	*config.syslog.setLogConfig*
8.0	*config.syslog.setState*
8.0	*config.syslog.show*
8.0	*config.system.contact*
8.0	*show.epFrameLog.disableTrigger*
8.0	*show.epFrameLog.setTrigger*
8.0	*show.fabric.traceRoute*
8.0	*show.port.opticData*
8.0	*show.port.opticHealth*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
8.0	*show.snmp.accessTable*
8.0	*show.snmp.targetTable*
8.0	*show.snmp.userTable*
8.0	*show.snmp.V3GroupTable*
8.0	*show.snmp.viewTable*
8.0	*show.syslog*
7.0	*config.features.NPIV*
7.0	*config.fencing.addPolicy*
7.0	*config.fencing.addPort*
7.0	*config.fencing.deletePolicy*
7.0	*config.fencing.removePort*
7.0	*config.fencing.setParams*
7.0	*config.fencing.setState*
7.0	*config.fencing.show*
7.0	*config.fencing.showTypeTable*
7.0	*config.ficonCUPZoning.addControlHost*
7.0	*config.ficonCUPZoning.deleteControlHost*
7.0	*config.ficonCUPZoning.setState*
7.0	*config.ficonCUPZoning.show*
7.0	*config.ficonMS.setMIHPTO*
7.0	*config.ficonMS.show*
7.0	*config.ip.lineSpeed*
7.0	*config.NPIV.maxPortIDs*
7.0	*config.NPIV.setState*
7.0	*config.NPIV.show*
7.0	*config.openSysMS.setHostCtrlState*
7.0	*config.port.rxCredits*
7.0	*config.port.show*
7.0	*config.port.showPortAddr*
7.0	*config.port.swapPortByAddr*
7.0	*config.port.swapPortByNum*
7.0	*config.security.authentication.interface.api.outgoing*
7.0	*config.security.authentication.interface.api.sequence*
7.0	*config.security.authentication.interface.cli.sequence*
7.0	*config.security.authentication.interface.eport.outgoing*
7.0	*config.security.authentication.interface.eport.sequence*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
7.0	*config.security.authentication.interface.nport.outgoing*
7.0	*config.security.authentication.interface.nport.sequence*
7.0	*config.security.authentication.interface.osms.outgoing*
7.0	*config.security.authentication.interface.osms.setKey*
7.0	*config.security.authentication.interface.serial.enhancedAuth*
7.0	*config.security.authentication.interface.show*
7.0	*config.security.authentication.interface.web.sequence*
7.0	*config.security.authentication.port.override*
7.0	*config.security.authentication.port.show*
7.0	*config.security.authentication.RADIUS.attempts*
7.0	*config.security.authentication.RADIUS.deadtime*
7.0	*config.security.authentication.RADIUS.deleteServer*
7.0	*config.security.authentication.RADIUS.server*
7.0	*config.security.authentication.RADIUS.show*
7.0	*config.security.authentication.RADIUS.timeout*
7.0	*config.security.authentication.switch.setSecret*
7.0	*config.security.authentication.user*
7.0	*config.security.authentication.user.add*
7.0	*config.security.authentication.user.delete*
7.0	*config.security.authentication.user.modify*
7.0	*Command example*
7.0	*config.security.authentication.user.show*
7.0	*config.security.ssh.resetKeys*
7.0	*Command example*
7.0	*config.security.ssh.show*
7.0	*config.security.switchAcl.addRange*
7.0	*config.security.switchAcl.deleteRange*
7.0	*config.security.switchAcl.setState*
7.0	*config.security.switchAcl.show*
7.0	*config.switch.apiState*
7.0	*perf.preferredPath.showPath*
7.0	*perf.thresholdAlerts.show*
7.0	*show.auditLog*
7.0	*show.epFrameLog.config*
7.0	*show.epFrameLog.filterClassFFrames*
7.0	*show.epFrameLog.noWrap*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
7.0	*show.epFrameLog.noWrap*
7.0	*show.epFrameLog.wrap*
7.0	*show.fabricLog.noWrap*
7.0	*show.fabricLog.wrap*
7.0	*show.fabric.principal*
7.0	*show.fencing.policies*
7.0	*show.ficonCUPZoning*
7.0	*show.ficonMS*
7.0	*show.NPIV.config*
7.0	*show.openSysMS.config*
7.0	*show.port.config*
7.0	*show.port.opticEDD*
7.0	*show.port.opticInfo*
7.0	*show.port.profile*
7.0	*show.port.showPortAddr*
7.0	*show.security.switchAcl*
7.0	*show.security.log*
6.1	*config.snmp.setFaMibVersion*
6.1	*config.snmp.setState*
6.1	*perf.preferredPath.clearPath*
6.1	*perf.preferredPath.setPath*
6.1	*perf.preferredPath.setState*
6.1	*perf.preferredPath.showPath*
6.1	*show.all*
6.1	*show.fabric.nodes*
6.1	*show.fabric.topology*
6.1	*show.linkIncidentLog*
6.1	*show.port.exit*
6.1	*show.preferredPath.showPath*
6.1	*show.syslog*
6.1	*show.thresholdAlerts.log*
5.3	*config.enterpriseFabMode.setState*
5.3	*config.features.openTrunking*
5.3	*config.ficonMS.setMIHPTO*
5.3	*config.NPIV.maxPortIDs*
5.3	*config.switch.ltdFabRSCN*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
5.3	*config.switch.webState*
5.3	*perf.openTrunking.backPressure*
5.3	*perf.openTrunking.congestionThresh*
5.3	*perf.openTrunking.lowBBCreditThresh*
5.3	*perf.openTrunking.setState*
5.3	*perf.openTrunking.show*
5.3	*perf.openTrunking.unresCongestion*
5.3	*perf.thresholdAlerts*
5.3	*show.openTrunking.config*
5.3	*show.openTrunking.rerouteLog*
4.0	*config.features.enterpriseFabMode*
4.0	*config.features.ficonMS*
4.0	*config.features.installKey*
4.0	*config.features.openSysMS*
4.0	*config.features.show*
4.0	*config.ip.ethernet*
4.0	*config.ip.show*
4.0	*config.port.blocked*
4.0	*config.port.fan*
4.0	*config.port.name*
4.0	*config.port.show*
4.0	*config.port.speed*
4.0	*config.port.type*
4.0	*config.security.fabricBinding*
4.0	*config.security.portBinding*
4.0	*config.security.switchBinding*
4.0	*config.snmp.authTraps*
4.0	*config.snmp.deleteCommunity*
4.0	*config.snmp.show*
4.0	*config.switch*
4.0	*config.switch.domainRSCN*
4.0	*config.switch.edTOV*
4.0	*config.switch.insistDomainId*
4.0	*config.switch.interopMode*
4.0	*config.switch.prefDomainId*
4.0	*config.switch.priority*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
4.0	*config.switch.raTOV*
4.0	*config.switch.rerouteDelay*
4.0	*config.switch.show*
4.0	
4.0	*config.system.date*
4.0	*config.system.description*
4.0	*config.system.location*
4.0	*config.system.name*
4.0	*config.system.show*
4.0	*config.zoning.activateZoneSet*
4.0	*config.zoning.addPortMem*
4.0	*config.zoning.clearZone*
4.0	*config.zoning.renameZoneSet*
4.0	*config.zoning.clearZone*
4.0	*config.zoning.renameZoneSet*
4.0	*config.zoning.deactivateZoneSet*
4.0	*config.zoning.deletePortMem*
4.0	*config.zoning.disableSplZoneSet*
4.0	*config.zoning.renameZoneSet*
4.0	*config.zoning.disableSplZoneSet*
4.0	*config.zoning.renameZoneSet*
4.0	*config.zoning.replaceZoneSet*
4.0	*config.zoning.setDefZoneState*
4.0	*config.zoning.showActive*
4.0	*config.zoning.showPending*
4.0	*maint.port.beacon*
4.0	*maint.port.reset*
4.0	*maint.system.beacon*
4.0	*maint.system.clearSysError*
4.0	*maint.system.ipl*
4.0	*maint.system.resetConfig*
4.0	*maint.system.setOnlineState*
4.0	*perf.class2*
4.0	*perf.class3*
4.0	*perf.clearStats*
4.0	*perf.errors*

TABLE 8 Commands and Releases (Continued)

E/OS Releases	Command
4.0	*perf.link*
4.0	*perf.traffic*
4.0	*show.eventLog*
4.0	*show.features*
4.0	*show.frus*
4.0	*show.ip.ethernet*
4.0	*show.loginServer*
4.0	*show.nameServer*
4.0	*show.nameServerExt*
4.0	*show.port.config*
4.0	*show.port.info*
4.0	*show.port.nodes*
4.0	*show.port.status*
4.0	*show.port.technology*
4.0	*show.preferredPath.showState*
4.0	*show.security.portBinding*
4.0	*show.security.switchBinding*
4.0	*show.switch*
4.0	*show.system*
4.0	*show.zoning*

B Commands and Corresponding Releases

Index

Symbols

", *12*
?, *16*

Numerics

60 characters in history log, *11*
80-column output, *12*

A

access control list, *93*
    adding a range, *93*
    delete a range, *94*
    disable, *95*
    enable, *95*
    show, *95*
access rights
    relationship to other products, *14*
active zoning configuration, *163*
add
    access control list, *93*
    alias to WWN, *21*
address
    port, *56*
AFD, *170*
    HDD report, *170*
    POM report, *170*
    show, *171*
Alert, *189*
alerts, threshold, *191*
alias, *20*
    activate pending, *21*
    add, *21*
    clear pending, *22*
    delete, *22*
    enabling CLI, *23*
    replacePending, *23*
    show active, *24*
    show pending, *25*
ASCII character set, *20*
asynchronous commands, *2*
attached
    fabric binding terminology, *81*
audit log
    show, *210*
authentication
    configuring E port, *63*, *64*
    configuring interface, *62*
    configuring N port, *64*
    configuring Open Systems, *66*
    configuring outgoing, *61*
    configuring port, *69*
    configuring sequence, *62*
    configuring serial, *67*
    configuring Web, *68*
    showing settings, *67*
authorization traps, SNMP, *113*

B

back pressure state
    OpenTrunking, *178*
backslash, *12*
BB_credits
    configuring, *53*
beaconing
    port, *166*
    unit, *167*
block port, *51*

C

cable, replacing, *18*
character set, *20*
class 2 counters, *172*
class 3 counters, *173*

CLI, *1*
command tree, *3*
ED-5000 Director, *17*
errors, handling, *16*
globally available commands, *3*
help, *16*
logging in or out, *12*
lost, *168*
navigation conventions, *2*
output, *12*
parameters, *12*
purpose, *1*
root> prompt, *10*
using, *1*
commaDelim command
globally available, *3*
command line interface, *1*
command tree, *3*
ED-5000, *17*
errors, handling, *16*
globally available commands, *3*
help, *16*
logging in or out, *12*
lost, *168*
navigation conventions, *2*
output, *12*
parameters, *12*
purpose, *1*
root> prompt, *10*
using, *1*
command tree, *3*
limitations on movements within, *11*
navigation of, *10*
Commands, *383*
commands
asynchronous, *2*
config, *19*
ED-5000, *17*
login, *13*
logout, *14*
maint, *165*
name server information, *241*
perf, *169*
periods in, *2*
show, *208*
that take effect immediately, *81, 153*
config command, *19*
configuration data, resetting, *165*
configuration, resetting, *168*
congestion
unresolved, *182*
congestion threshold
OpenTrunking, *178*
connection loss, ethernet, *18*
conventions
documentation, *2*
navigation, *2*
counter data, *172, 173*
counter threshold alert
activating, *188*
types, *189*
counter threshold alerts, *191*
CTA, *191*
CUP zoning, *38, 39*

D

data transfers, disruption of, *58, 138*
date and time, system, *146*
deactivate fabric binding, *84*
default values, resetting, *168*
default zone, *162*
delete
access control list, *94*
alias, *22*
preferred path, *183*
dependencies, *25*
disable
access control list, *95*
OpenTrunking, *180*
SNMP agent, *117*
disabling
enterprise fabric mode, *25*
documentation conventions, *2*
Domain ID
state, *132*
domain ID, port member
adding, *154*
deleting, *158*
domain RSCN state, *107, 110, 111, 112, 114, 115, 130*

E

e_d_tov, *108, 131*
E_port, setting, *60*
ED-5000 Director, *17*

Embedded Frame Log
show configuration, *211*
view, *213*, *217*
enable
access control list, *95*
OpenTrunking, *180*
SNMP agent, *117*
enabling, *26*
enterprise fabric mode, *25*, *26*
feature set, *27*
NPIV, *28*
enbling
FICON Management Server, *27*
Enterprise Fabric Mode
activating, *25*, *26*
deactivating, *25*, *26*
enterprise fabric mode, *26*
disabling, *25*
enabling, *25*
error counters, port, *175*
error light, system, clearing, *167*
escape character, *12*
ethernet attributes, *237*
ethernet cable, replacing, *18*
ethernet connection, loss of, *18*
event log, *218*
exit port
set, *184*

F

F frames
configuring logging, *213*
F_port, setting, *60*
fabric address notification (FAN)
setting state, *52*
fabric binding
activate, *82*
active configuration, *85*
active FBML
show, *85*
add members, *82*, *83*
deactivate, *84*
delete members, *84*
membership list, *83*
delete member, *84*
online state functions, *81*
pending configuration
activate, *82*
add attached members, *82*
pending FBML
show, *86*
replace pending, *85*
replace pending FBML, *85*
security, *80*
show, *268*
show pending, *86*
terms
attached, *81*
local, *81*
unattached, *81*
fabric binding membership list
active, *85*
add member, *83*
clear, *83*
deactivate, *84*
delete member, *84*
pending
show, *86*
replace pending FBML, *85*
fabric log
view, *222*, *223*
fabric nodes
list, *224*
show, *224*
fabric topology
list, *228*
show, *228*
factory settings, resetting, *165*, *168*

feature
enabling, *27*
Enterprise Fabric Mode, *25, 26*
FICON Management Server, *27, 40*
list, *231*
NPIV, *28*
Open Systems Management Server, *28, 50*
OpenTrunking, *29, 180*
SANtegrity, *25, 26*
show, *231*
feature key
NPIV, *28*
feature keys, *27*
resetting, *168*
features
preferred path, *182*
fencing policies
show, *232*
Fibre Alliance MIB
SNMP, *117*
FICON
enabling management server, *27*
FICON CUP
show zoning, *234*
zoning, *38, 39*
FICON Management Server, *27, 40*
FICON MS
show, *234*
ficonms, *27, 40*
FRU information, *235*

G

G_port, setting, *60*
gateway address, *42*
globally available commands, *3*
graphical user interface, *1*
GUI, *1*

H

help command, *16*
history log, *11*
clearing, *11*
HTTP, *1*

I

inactive operational state, *264*
inactive state reasons, *264*
insistent Domain ID
state, *132*
interactive interfaces, *1*
interoperability mode, *132*
invalid attachment state reasons, *264*
IP address, ethernet, *42*
IP configuration, showing, *43, 44*
IP line speed, ethernet, *42*
IPL, *168*

K

keys
for feature sets, *27*
resetting, *168*

L

Latin-1 character set, *20*
limitations, history log, *11*
limited fabric RSCN, *134*
link counters, *176*
link incident log, *237*
link sequence counts, *190*
local
fabric binding terminology, *81*
log
Embedded Frame
settings, *213*
threshold alert, *287*
view, *218*
logging in, *12*
logging out, *12*
logical link errors, *191*
login command, *13*
globally available, *3*
login server, *238*
logout command, *14*
globally available, *3*
low BB credit threshold, *179*

M

maint command, *165*
management server
    enabling, *27*
Management Style
    FICON, *27*
membership list
    fabric binding, *84*
        add attached, *82*
        add member, *83*
        clear, *83*
    switch binding, *96*

N

name server, *239*, *241*
names, for ports, *52*
navigating the command tree, *10*
    limitations, *11*
navigation conventions, *2*
NPIV
    configuring port IDs, *44*, *45*
    disable, *28*
    enable, *28*
    enabling, *28*
    set state, *28*
    setting state, *46*
    showing configuration, *46*
NSTools, *47*
    clear snapshot, *47*
    save snapshot, *48*
    show snapdiff, *48*
    show snapshot, *49*
null strings, *12*
NV-RAM configuration parameters, reset, *168*

O

offline, setting switches for configuration, *108*
Open Systems
    setting state, *50*
Open Systems Management Server, *28*, *50*
OpenTrunking
    back pressure state, *178*
    congestion threshold, *178*
    low BB credit threshold, *179*
    show, *180*
        configuration, *246*
        reroute log, *247*
    state, *29*, *180*
    unresolved congestion, *182*
operational state, *264*
OSMS state, *28*, *50*
output, *12*
    order of displayed values, *10*

P

parameters, *12*
passwords
    format, *13*
perf command, *169*
performance alerts, *191*
performance services, *169*
periods in command names, *2*
physical link errors, *190*

port
address, show, *261*
beaconing, *166*
binding, *87*, *270*
binding, state, *87*
block, *51*
configuration, *248*
configuration, show, *259*
configuring BB_credits, *53*
configuring WWN, binding, *89*
error counters, *175*
IDs, NPIV, *44*, *45*
information, *251*
link counters, *176*
name, *52*
nodes, *253*
optical diagnostics, *255*
port statistics, *174*
port technology information, *265*
QPM mode setting, *52*
resetting, *166*
show configuration, *248*
show exit, *249*
show nodes, *253*
show optic, *257*
showing address configuration, *56*
showing authentication state, *70*
showing configuration, *54*
speed, *58*
statistics, clearing, *174*
status, *262*
swapping, *59*
threshold alert, *192*, *193*
traffic counters, *207*
type, *60*
port binding state, *87*
port number, zone member
adding, *154*
deleting, *158*
port statistics, resetting, *174*
preferred domain ID, *134*
preferred path
clear, *183*
delete, *183*
destination, *185*, *266*
disable, *185*
enable, *185*
feature overview, *182*
set exit port, *184*
show, *266*
show exit port, *250*
show path, *185*
show state, *187*, *188*
source port, *185*, *266*
state, *185*
principal switch, *135*
priority, of switches, *135*

Q

QPM
setting mode, *52*
quotation marks
for spaces, *12*
in strings, *12*

R

r_a_tov, *135*
RADIUS server
adding, *72*
configuring deadtime, *71*
configuring timeout, *74*
deleting, *72*
showing configuration, *73*
range
access control list, *93*, *94*
reroute log, OpenTrunking, *247*
rerouting delay, *136*
root> prompt, *10*
RSCN
fabric, *134*

S

SANtegrity
Enterprise Fabric Mode, *25*, *26*
scripting environments, *1*

secret
setting, *75*
secrets
format, *13*
secure shell
keys, *91*
set state, *92*
show state, *92*
security
adding RADIUS server, *72*
adding users to database, *75*
configuring, *61*
configuring authentication interface, *62*
configuring authentication sequence, *62*
configuring E port authentication, *63*, *64*
configuring N port authentication, *64*
configuring Open Systems authentication, *66*
configuring outgoing authentication, *61*
configuring port state, *69*
configuring RADIUS server deadtime, *71*
configuring serial authentication, *67*
configuring transmission attempts, *70*
configuring users, *75*
configuring Web authentication, *68*
deleting RADIUS server, *72*
deleting users from database, *77*
fabric binding, *80*
activate, *82*
active configuration, *85*
add members, *82*, *83*
deactivate, *84*
delete members, *84*
replace pending, *85*
show pending, *86*
modifying users, *77*
port binding, *87*
reset SSH keys, *91*
set SSH renegotiation MB, *91*
set SSH state, *92*
setting secret, *75*
setting user role, *79*
show SSH state, *92*
showing port, *70*
showing RADIUS server, *73*
showing state, *67*
showing user, *79*
switch binding, *96*
adding member, *97*
deleting member, *97*
setting state, *98*
showing configuration, *98*
timeout
RADIUS server, *74*
security log, *269*
segmented E_Port, *264*
segmented E_port
state reasons, *264*
setting online or offline, *169*
settings
threshold alert settings, *205*

show, *280*
access control list, *95*
all, *209*
ethernet attributes, *237*
event log, *218*
fabric binding, *268*
fabric nodes, *224*
fabric ping, *225*
fabric show route table, *226*
fabric topology, *228*
fabric trace route, *229*
features list, *231*
fencing policies, *232*
FICON CUP zoning, *234*
FICON MS, *234*
FRU information, *235*
link incident log, *237*
login server, *238*
name server, *239*
nameserver FC4 types, *242*
open trunking configuration, *246*
OpenTrunking
configuration, *246*
rerouteLog, *247*
OpenTrunking information, *180*
port address, *261*
port binding for all ports, *270*
port configuration, *248, 259*
port exit, *249*
port information, *251*
port nodes, *253*
port optic, *257*
port optical diagnostics, *255*
port status, *262*
port technology information, *265*
preferred path, *266*
preferred path exit port, *250*
security log, *269*
switch access control list, *271*
switch attributes, *281*
switch binding, *272*
Switch Binding Membership List, *99*
system attributes, *283*
threshold alert list, *285*
threshold alert log, *287*
threshold alert settings, *205*
WWN, *226*
show commands
active zoning configuration, *163*
all, *209*
configuration for port, *54*
features, *30*
order of output, *10*
pending zoning configuration, *163, 164*
port
show binding, *88*
show branch, *208*
SNMP configuration
config.snmp.show, *118*
snmp.show, *279*
switch configuration, *139*
system configuration, *148, 149*
SNMP
authorization traps, *113*
community
adding, *106*
deleting, *114*
disable agent, *117*
enable agent, *117*
Fibre Alliance MIB version, *117*
send test trap, *116*
set state, *117*
spaces, quotation marks required, *12*
speeds
port, *58*
switches, *138*
state
back pressure, *178*
OpenTrunking, *29, 180*
setting NPIV, *46*
SNMP, *117*
Zone Flex Pars, *125*
statistic table, threshold alert, *196*
statistics, port, clearing, *174*
strings, null, *12*
strings, quotation marks in, *12*
subnet mask, *42*
summed sets, *190*
Supported, *154*
swap ports
by address, *59*
by number, *59*
switch attributes, displaying, *281*
Switch Binding
add SBML member, *97*
configuration, *96*
delete SBML member, *97*
show configuration, *98*

switch binding, *272*
adding member, *97*
delete member, *97*
online state functions, *96*
set state, *98*
show configuration, *98*
show SBML, *99*
Switch Binding Membership List, *99*
add member, *97*
delete member, *97*
overview, *96*
show, *99*
switches, *169*
banner, *126*
banner text, *126*
set CLI state, *127*
set web state, *128*
show, *128*
configuring IP address, *42*
configuring IP line speed, *42*
configuring, set offline, *108*
domain ID offset, *129*
e_d_tov, *108, 131*
event log, *218*
FRU information, *235*
interoperability mode, *132*
IPL, *168*
login server database, *238*
name server database, *239, 241*
preferred domain ID, *134*
principal, *135*
priority, *135*
r_a_tov, *135*
rerouting delay, *136*
security log, *269*
showing LAN configuration, *43, 44*
speed, *138*
system contact, *145*
system description, *146*
system location, *147*
system name, *147*
system attributes, displaying, *283*
system contact attribute, *145*
system date and time, *146*
system description, *146*
system error light, clearing, *167*
system location, *147*
system name, *147*

T

Telnet client session, *1*
connection, loss of, *18*
threshold alert
activate, *198*
add alert, *191*
add port, *201*
add throughput alert, *200*
alert list, *285*
counter
setting, *194*
deactivate, *198*
delete alert, *197*
disable, *198*
enable, *198*
list, *285*
log, *287*
name, *196*
parameters, *195, 204*
port
add, *192, 201*
remove, *193, 202*
remove port, *202*
set parameters, *204*
settings
show, *205*
show, *198, 205*
show utilization types, *206*
statistic table, show, *196*
throughput
add alert, *200*
trigger
percentage, *204*
trigger type, *203*
utilization percentage, *204*
utilization type, *203*
utilization types, *206*
threshold alerts
overview, *191*
summed sets, *190*
Throughput, *189*
throughput alert
add, *200*
port, *201, 202*
set parameters, *204*
show settings, *205*
show utilization types, *206*
utilization percentage, *204*
utilization type, *203*

Throughput Threshold Alert
activating, *189*
throughput threshold alert, *191*
types, *189*
time, system, *146*
traffic counters, *207*
traversing the command tree, *10*
trunking
congestion, *178, 182*
TTAs, *191*
types, port, *60*

U

UDP, *107, 119*
unattached
fabric binding terminology, *81*
unit beaconing, *167*
unresolved congestion
OpenTrunking, *182*
up-arrow command, *11*
user
adding to database, *75*
configuring, *75*
deleting from database, *77*
modifying, *77*
password expiration time, *78*
setting role, *79*
showing, *79*
user access rights
relationship to other products, *14*
user datagram protocol, *107, 119*
utilization type
threshold alert, *203*

V

view
logs, *213, 217, 222, 223*

W

web-based interface, *1*
work area, *153*
world-wide name members
adding, *155*
deleting, *159*
wrap count, *172, 173*
WWN
port binding, *89*
show, *226*
WWN members
adding, *155*
deleting, *159*

Z

zone
adding, *156*
default state, *162*
deleting, *159, 160*
members
adding by port, *154*
adding by WWN, *155*
deleting by port, *158*
deleting by WWN, *159*
renaming, *160*
Zone Flex Pars
zoning state, *125*
zone members
clearing, *157*
domain ID
adding, *154*
deleting, *158*
zone set
activating to fabric, *153, 154*
clearing, *157*
deactivating, *157*
renaming, *161*
replacing, *162*
temporary copy, *153*
zone sets and zones
displaying, *154*
zoning
configuring, *153*
FICON CUP, *38, 39*
show FICON CUP, *234*
Zone Flex Pars state, *125*
zoning configuration
active, display, *163*
pending, display, *163, 164*